Universitat Autònoma de Barcelona

www.uoc.edu

Universitat Rovira i Virgili

Máster Interuniversitario en Seguridad de las TIC (MISTIC)

TRABAJO FINAL DE MASTER

PLAN DIRECTOR DE SEGURIDAD

CONSULTOR: Antonio José Segovia Henares.

ALUMNO: Ronald Andrés Téllez Vivanco.

2013

INDICE

Pág.

INDICE DE FIGURAS

Pág.

1. INTRODUCCION

El presente Trabajo Tic Solution, situado en la ciudad de Cartagena de Indias, COLOMBIA, TIC SOLUTION es un establecimiento público, con financiamiento propio derivado de los aportes parafiscales de los empresarios, que ofrece instrucción gratuita a millones de personas que se benefician con programas de formación complementaria y titulada y jalona el desarrollo tecnológico para que las empresas del país sean altamente productivas y competitivas en los mercados globalizados.

Busca la capacitación técnica del recurso humano; forma personas para vincularlas al mercado laboral, empleadas o subempleadas; y realiza actividades de desarrollo empresarial, comunitario y tecnológico.

1.1 Selección de la empresa:

TIC SOLUTION

1.2 Misión

El TIC SOLUTION está encargado de cumplir la función que le corresponde al Estado de invertir en el desarrollo social y técnico de los trabajadores colombianos, ofreciendo y ejecutando la formación profesional integral, para la incorporación y el desarrollo de las personas en actividades productivas que contribuyan al desarrollo social, económico y tecnológico del país.

1.3 Visión

En el 2020, el TIC SOLUTION será una Entidad de clase mundial en formación profesional integral y en el uso y apropiación de tecnología e innovación al servicio de personas y empresas; habrá contribuido decisivamente a incrementar la competitividad de Colombia a través de:

- Aportes relevantes a la productividad de las empresas.
- Contribución a la efectiva generación de empleo y la superación de la pobreza.

- Aporte de fuerza laboral innovadora a las empresas y las regiones.
- Integralidad de sus egresados y su vocación de servicio.
- Calidad y estándares internacionales de su formación profesional integral.
- Incorporación de las últimas tecnologías en las empresas y en la formación profesional integral.
- Estrecha relación con el sector educativo (media y superior).
- Excelencia en la gestión de sus recursos (humanos, físicos, tecnológicos y financieros).

1.4 Organigrama.

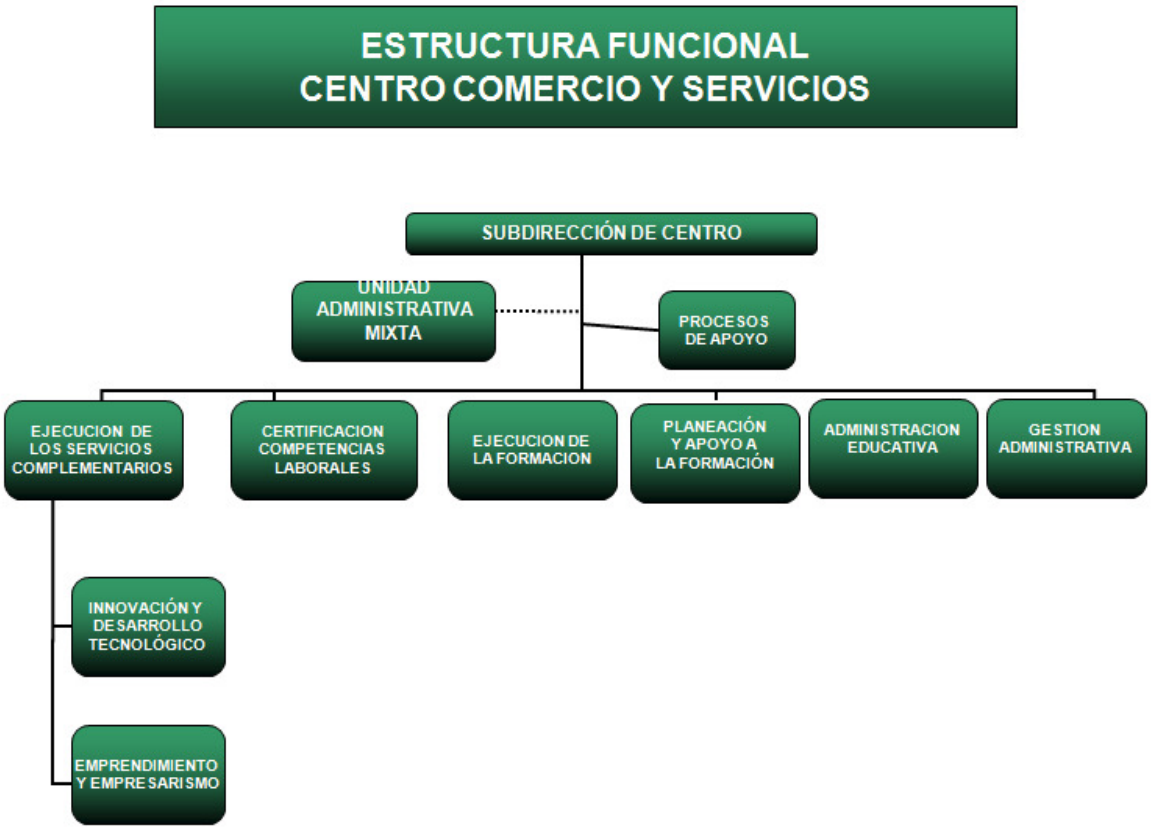


Figura 1. Organigrama

2. OBJETIVOS

2.1 Objetivo General

Diseñar un sistema para gestionar la seguridad de los activos de información (SGSI) basado en los estándares de la ISO 27001, y utilizando la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT en el Sistema De Información de TIC SOLUTION, permitiendo Analizar, replantear, proponer y diseñar políticas, planes y controles pertinentes para proporcionar una solución a los requerimientos de seguridad y protección de la información.

2.2 Objetivos Específicos

- Puntualizar y establecer el alcance del SGSI en TIC SOLUTION.
- Identificar activos y la importa de estos para la organización y entender el esquema de trabajo o funciones o que realizan.
- Determinar la dependencia entre los activos.
- Determinar el Valor los activos de información para TIC SOLUTION y determinar su la postura en términos de disponibilidad, confidencialidad, integridad y autenticidad.
- Identificar las falencias, amenazas y riesgos a los cuales están expuestos los activos de información, determinando el impacto que estos ocasionarían al centro.
- Determinar las políticas y los controles pertinentes como medida de seguridad para la preservación de la integridad, confidencialidad y disponibilidad permitiendo gestionar los riesgos identificados.
- Realizar la estructura documentaría del SGSI con las políticas, guías y controles y procedimientos aplicados.

3. FORMULACIÓN DEL PROBLEMA

¿De qué forma se puede diseñar un sistema que garantice la gestión de la seguridad y protección de los activos de información, supliendo los requerimientos, deficiencias y

vulnerabilidades tanto de carácter físico como lógico para el sistema de información de TIC SOLUTION?

4. JUSTIFICACIÓN

El centro TIC SOLUTION por ser una de las más grandes entidades públicas prestadoras del servicio de capacitación Técnica y tecnóloga profesional en el departamento de Bolívar, posee una gran infraestructura donde se manejan flujos considerables de información tanto de manera física como sistematizada y de carácter vital para su funcionamiento. Por tal motivo se hace necesario que se implementen, mejoren y normalicen las pautas que permitan realizar un análisis de los componentes de la organización, que consiste en diseño de normas, acciones y medidas que permitan dar seguridad a todos estos elementos.

La información, los procesos, sistemas y las redes se constituyen en importantes recursos de la empresa. La confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial. La dependencia de las organizaciones respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a seguridad.

Uno de los factores que intervienen en gran medida dentro de los elementos de la seguridad son los relacionados con la tecnología informática, vinculado con este elemento se puede encontrar un concepto que permite realizar un análisis sobre la entidad para brindar la seguridad necesaria.

El diseño de un Sistemas de Gestión de la Seguridad de la Información (SGSI) que propone proyecto, es una alternativa de solución que permite utilizar los elementos necesarios tanto técnicos y prácticos como conceptuales para que los requerimientos de seguridad expuestos y observados en la entidad sean satisfechos, esto se realiza por medio del diseño de un conjunto adecuado de controles, que abarca políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software. Estos controles se establecen para garantizar que se logren los objetivos específicos en la seguridad de la organización y lograr la preservación de las siguientes características o pilares sobre los cuales se basa la calidad del servicio.

5. DEFINICION DEL ALCANCE

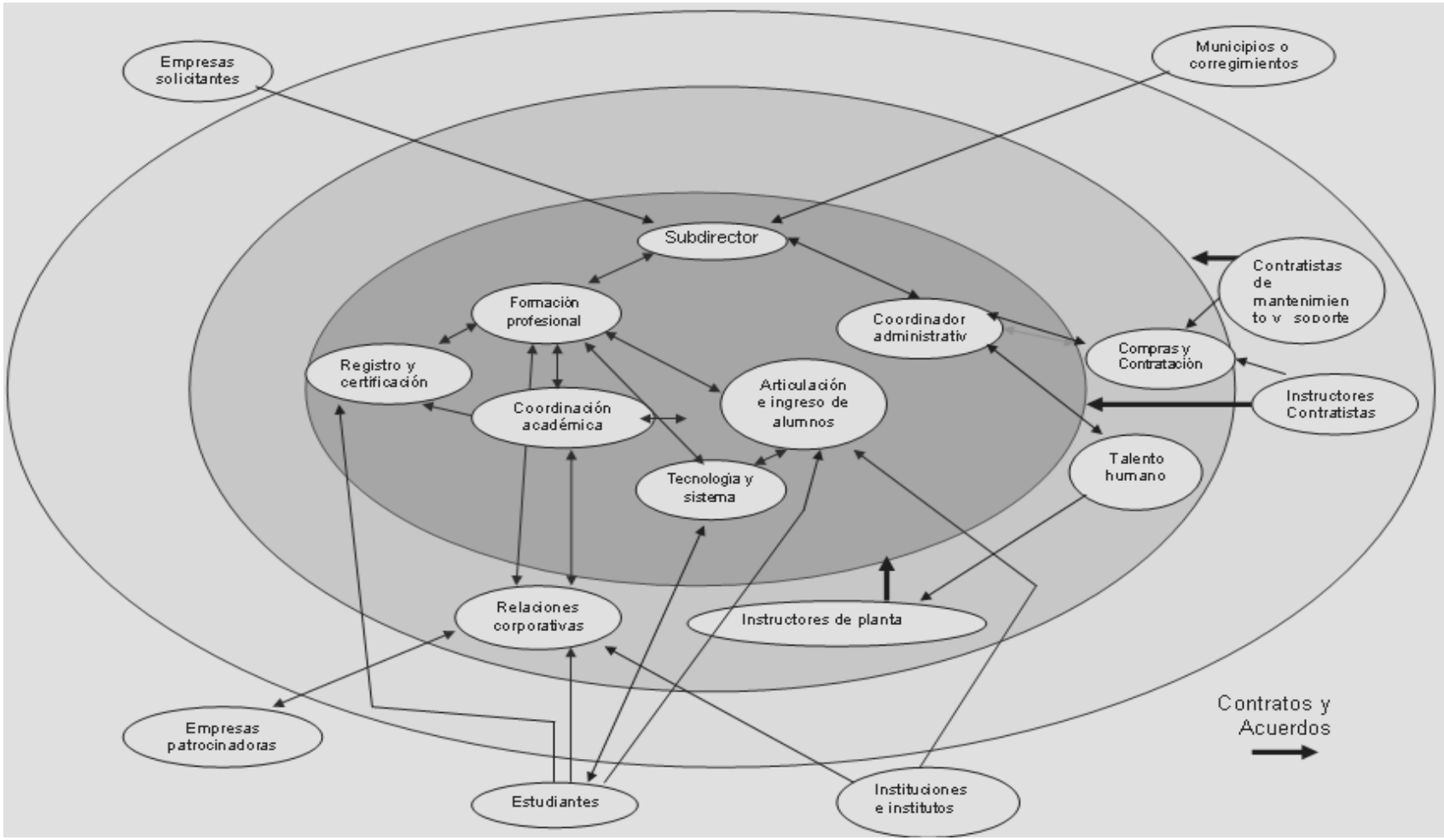


Figura 2. Definición del alcance del plan directo

El Consejo Directivo definió que el alcance del plan director se enfocara en todos los departamentos o procesos que se encuentran en la elipse del centro con sus correspondientes activos y que los departamentos o procesos que están en las elipses externas, serán tenidos en cuenta dependiendo del flujo de la información que manejen y de la dependencia de los activos con relación a la lógica del negocio.

6. FASES DEL PLAN DIRECTOR

El plan director de seguridad tiene por misión el establecimiento de políticas y controles en el contexto de la organización. Este se basa en un conjunto de documentos y herramientas que demuestran y ayudan a realizar la gestión de la seguridad como son la ISO 27001 y la metodología para el análisis y gestión de riesgos de los sistemas de información MAGERIT.

El plan director de seguridad se compone de las siguientes fases:

1. Definición del ámbito o alcance: Donde se define y se delimita las áreas de aplicabilidad de sistema de Gestión.

2. Análisis Gap*:* Fase donde se chequea y se realiza un balance de las falencias que presenta la organización en cuanto a seguridad

3. Identificación de los activos de información: Fase que se encarga de definir e identificar todo aquello que genera un valor para la organización el sistema de información.

4. La valorización de los activos de información*:* En esta face se define cuanto valor representa el activo para la organización basado en los criterios de disponibilidad, integridad y confidencialidad

5. Análisis de riesgo: Etapa donde se valora el impacto y los riegos de las amenazas latentes en la organización.

6. Definición de políticas: Es la definición de los lineamientos específicos para gestionar la seguridad de la información

7. Selección de controles: Son los mecanismos utilizados para ejecutar las políticas de seguridad.

8. Definición de la estructura documentaria: Donde se definen y establecen los documentos que apoyaran los controles de seguridad.

7. REQUERIMIENTOS NORMATIVOS

Para la realización del Plan director de seguridad informática se tendrá en cuenta el estándar internacional ISO/IEC 27001 y la guía de buenas prácticas ISO 27002:2005, este estándar se basa en la gestión de riesgos y subministra las pautas necesarias a considerar para la implementación de controles y la creación de políticas de seguridad bajo el foque PHVA, tomando elementos que puedan estructurarlo de forma adecuada. Un sistema de gestión de esta índole está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

Las fases son las siguientes:

- La Fase de planificación: esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).

- La Fase de implementación: esta fase implica la realización de todo lo planificado en la fase anterior.

- La Fase de revisión: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos “canales” y verificar si los resultados cumplen los objetivos establecidos.

- La Fase de mantenimiento y mejora: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

7.1 Documentos de ISO 27001.

La norma ISO 27001 requiere los siguientes documentos:

- Alcance del SGSI
- Política del SGSI
- Procedimientos para control de documentación, auditorías internas y procedimientos para medidas correctivas y preventivas
- Todos los demás documentos, según los controles aplicables
- Metodología de evaluación de riesgos
- Informe de evaluación de riesgos
- Declaración de aplicabilidad
- Plan de tratamiento del riesgo
- Registros.

7.2 Documentos de ISO 27002

Introducción.

Desde el 1 de Julio de 2000, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.

En España ya se encuentra traducida desde el 2009: UNE ISO/IEC 2700. Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO

17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.

7.3 Directrices

ISO 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

La seguridad de la información se define en el estándar como "la preservación de la Confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la Información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2005 del estándar incluye las siguientes secciones principales:

- Introducción: Conceptos generales de seguridad de la información y SGSI.
- Campo de aplicación: Se especifica el objetivo de la norma.
- Términos y definiciones: Breve descripción de los términos más usados en la norma.
- Estructura del estándar: Descripción de la estructura de la norma. Evaluación y tratamiento del riesgo: Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- Política de Seguridad: Documento de política de seguridad y su gestión.
- Aspectos Organizativos: Organización interna; organización externa
- Gestión de Activos: Responsabilidad sobre los activos; clasificación de la información.
- Recursos Humanos: Anterior al empleo; durante el empleo; finalización o cambio de empleo.
- Física y Ambiental: Áreas seguras; seguridad de los equipos.
- Comunicaciones y Operaciones: Procedimientos y responsabilidades de operación; gestión de servicios de terceras partes; planificación y aceptación

del sistema; protección contra software malicioso; backup; gestión de seguridad de redes; utilización de soportes de información; intercambio de información y software; servicios de comercio electrónico; monitorización.

- Control Accesos: Requisitos de negocio para el control de accesos; gestión de acceso de usuario; responsabilidades del usuario; control de acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.

- Adquisición, desarrollo y mantenimiento de sistemas: Requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas.

- Gestión de incidentes: Comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.

- Gestión Continuidad de negocio: Aspectos de la seguridad de la información en la gestión de continuidad del negocio.

- Cumplimiento legal: Con los requisitos legales; políticas de seguridad y estándares de conformidad y conformidad técnica; consideraciones sobre la auditoría de sistemas de información.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación.

El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

La norma Iso/IEC 27001, contiene los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información. Esta norma recoge los componentes del sistema, los documentos mínimos que deben formar parte de él y los registros que permitirán evidenciar el buen funcionamiento del sistema. Asimismo, especifica los requisitos para implantar controles y medidas de seguridad adaptados a las necesidades de cada organización. Con Esta norma serán certificados los Sistemas de Gestión de Seguridad de la Información en la institución. El estándar aplica para cualquier organización sin importar el tamaño y a su vez define 11 **dominios de control** que cubren por completo la Gestión de la Seguridad de la Información:

1. Política de seguridad
2. Organización de la información de seguridad
3. Administración de recursos
4. Seguridad de los recursos humanos
5. Seguridad física y del entorno
6. Administración de las comunicaciones y operaciones
7. Control de accesos
8. Adquisición de sistemas de información, desarrollo y Mantenimiento
9. Administración de los incidentes de seguridad.
10. Administración de la continuidad de negocio.
11. Cumplimiento (legales, de estándares, técnicas y auditorias).

Para realizar el análisis de riesgos se hará uso de MARGERIT, Es una metodología que brinda las pautas, las técnicas y los métodos necesarios para auditar sistemas de información que manejan medios electrónicos, informáticos, telemáticos, e información mecanizada en sus operaciones.

MARGERIT es un método de compuesto por tres fases para implementar una solución de SGSI como lo son:

1. **Planificación:** En esta parte se identifican y se definen los objetivos, la pertinencia, los requerimientos y las consideraciones necesarias para realizar el proyecto.

2. **Análisis de riesgos:** En esta fase se identifican todos y cada uno de los activos a tratar en la organización, sus dependencias y las amenazas a las que están expuestos. Igualmente se tiene en cuenta el impacto, la degradación y la frecuencia que tienen cada una de estas amenazas en el activo, analizando las salvaguardas existentes para mitigar este efecto.

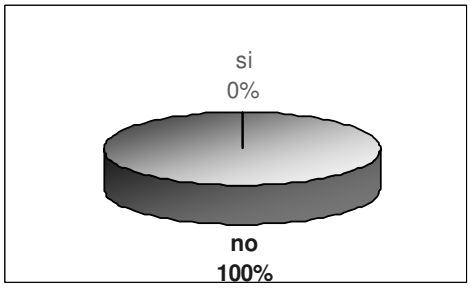
3. **Gestión de riesgos:** Se buscan los mecanismos y las salvaguardas apropiadas y oportunas para mitigar el impacto y el riesgo de cada una de las amenazas a niveles aceptables través del diseño de un plan de seguridad.

8. ANALISIS DIFERENCIAL ISO 27001

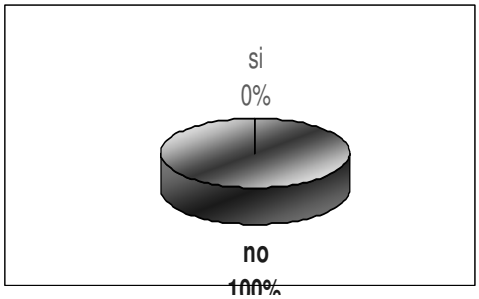
ANEXO ANALISIS GAP

Se realiza un análisis del nivel de seguridad con respecto a la ISO 27001+ISO27002

1) Políticas de seguridad



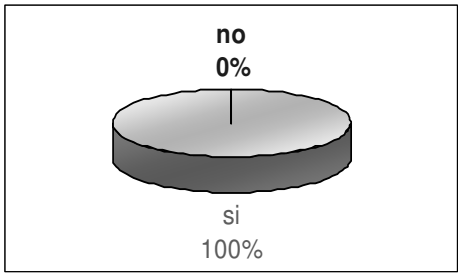
2) Seguridad de la organización

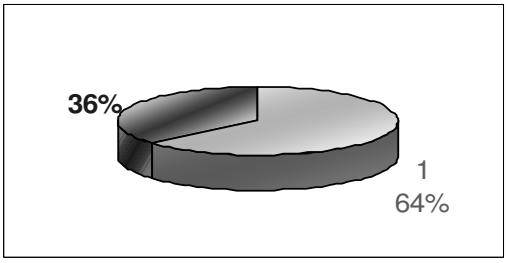


1) Se presenta este diagnóstico debido a que en el Tic Solution hay una carencia de políticas de seguridad, medios para proteger la información y controles regulares para verificar la efectividad de las mismas.

2) Hay ausencia de mecanismos y procedimientos estructurados con responsabilidades y obligaciones detalladas contra hechos que afecten la seguridad organizacional, de igual forma faltan programas de formación en seguridad para los empleados.

3) Clasificación del control de activos **4) Seguridad física y del Entorno**

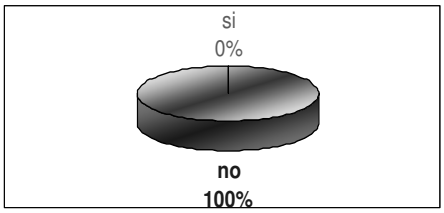


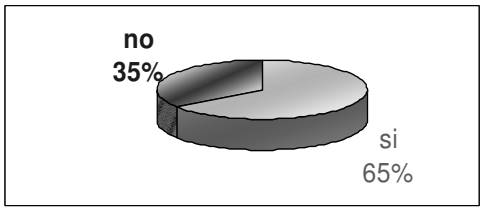


3) No existen procedimientos para clasificar y etiquetar la información y gran variedad de activos. Aunque actualmente se cuenta con un Inventario este no está actualizado ni organizado en forma eficiente.

4) En el Tic Solution los perímetros de seguridad física no cumplen con todas las normas necesarias; No existe una protección eficaz contra fallos en la alimentación eléctrica y los mecanismos para asegurar la disponibilidad e integridad de todos los equipos son deficientes.

5) Seguridad del personal **6) Gestión de comunicaciones y operaciones**

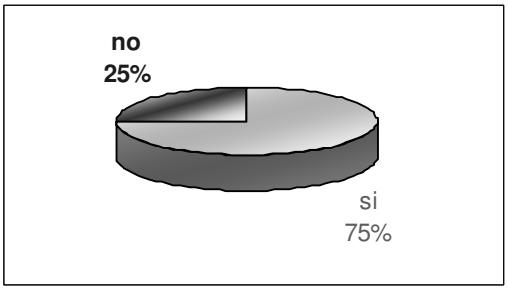




5) Actualmente no se tienen claramente definidos los Procedimientos, responsabilidades y roles de seguridad a seguir en caso de incidente. De la misma forma falta claridad para efectos de seguridad en cuanto a la selección y baja del personal.

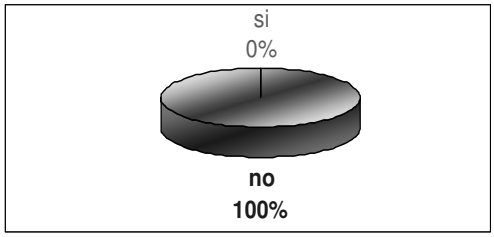
6) Falta claridad a la hora determinar las responsabilidades pertinentes para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad. De la misma forma las medidas para proteger la confidencialidad e integridad de información, como también los controles para realizar la gestión de los medios informáticos poseen falencias significativas.

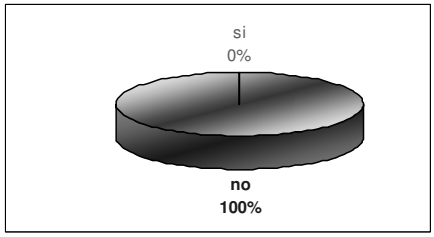
7) Control de accesos



7) Existen fallas en las políticas de control de accesos, para la restricción y asignación de privilegios en entornos multi-usuario. Esto se produce por que no se realiza la revisión y evaluación de los derechos de acceso para los mismos.

8) Desarrollo y mantenimiento de sistemas 9) Comunicación de eventos



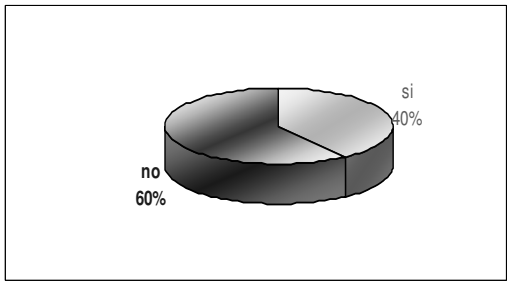


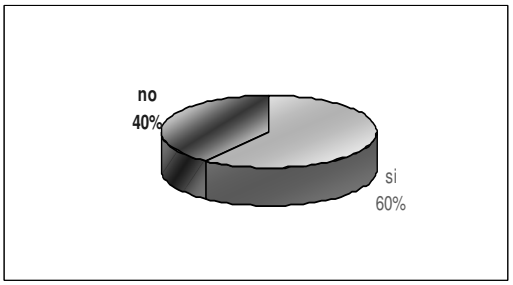
8) Son casi inexistentes las medidas para controlar las vulnerabilidades de los equipos, los sistemas operativos y los ficheros del sistema.

No se tienen mediadas de seguridad en el proceso desarrollo, testing y soporte.

9) Actualmente no existen registros ni mecanismos para comunicar los eventos e incidentes de seguridad. De igual manera no están definidas las responsabilidades antes un incidente y el procedimiento formal de respuesta.

10) Gestión de la continuidad del negocio **11)** Conformidad

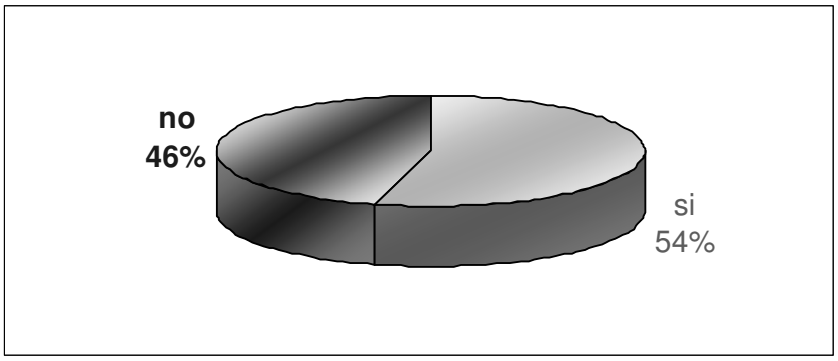




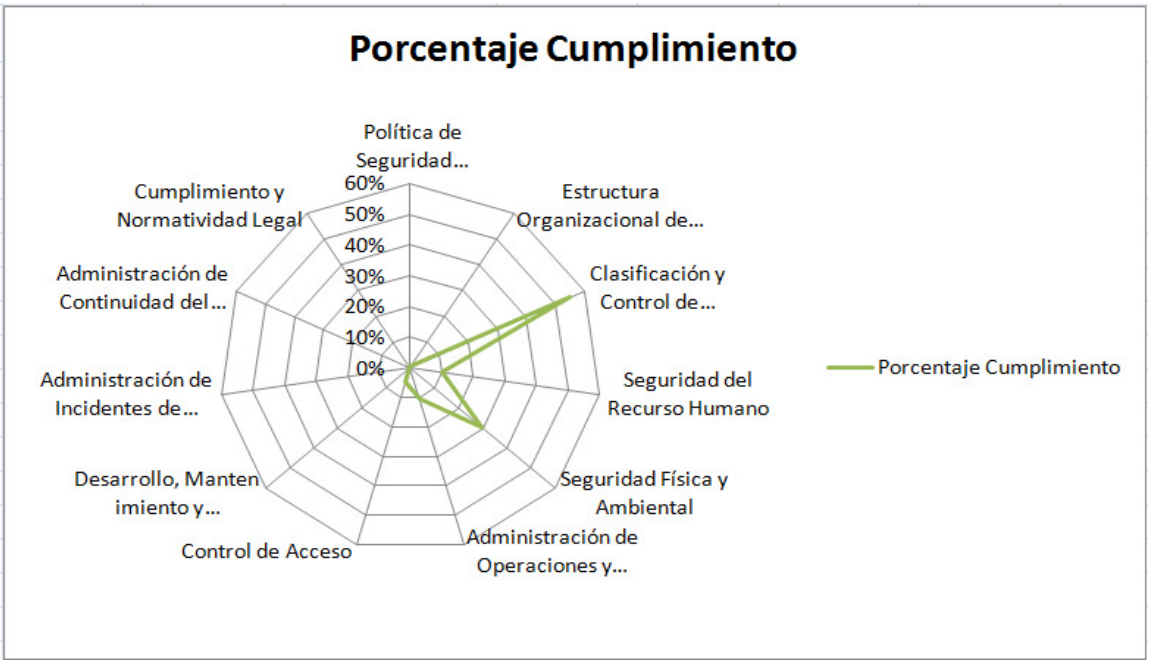
10) Son deficientes las pruebas y procedimientos para el mantenimiento y reevaluación de los planes de continuidad del negocio. Esto se debe a que son pocos los procesos para la gestión del análisis de impacto de incidentes y amenazas.

11) Son muy pocos los procedimientos para la revisión de las políticas de seguridad y las conformidades técnicas

RESULTADO GENERAL



Se evidencia que el cumplimiento de la norma ISO27001 y sus dominios cumplen en un 54% lo que videncia que la empresa está expuesta a vulnerabilidades en un 46%.



Observamos el nivel de cumplimiento de la norma ISO27001 en cada uno de los dominios, queda evidenciado los porcentajes de cumplimiento que tiene cada dominio respecto a la norma.

Anexo archivo análisis Diferencial

9. ESQUEMA DOCUMENTAL

9.1 Política de Seguridad

Esta Política de Seguridad de la Información del SGSI se ha desarrollado para garantizar la confidencialidad, integridad y disponibilidad de la información y de los de los procesos, Al implementar esta política las personas involucradas, tanto empleados como proveedores, deben garantizar la protección de los procesos, la reputación y la mejora continua. Encontrará definición de la política en el anexo Política de seguridad.

9.2 Gestión de Roles y Responsabilidades

El Sistema de Gestión de Seguridad de la Información tiene que estar compuesto por un equipo que se encargue de crear, mantener, supervisar y mejorar el Sistema. Este equipo de trabajo, conocido habitualmente como Comité de Seguridad, debe estar compuesto al menos por una persona de Dirección, para que de esta manera las decisiones que se tomen puedan estar respaldadas por alguien de Dirección. La definición de roles y responsabilidades lo encontrara en anexo Gestión de Roles y Responsabilidades.

9.3 Fases del proyecto

El desarrollo del plan director se ha organizado en cuatro fases que se describen en el siguiente grafico junto con las principales actividades de cada uno:

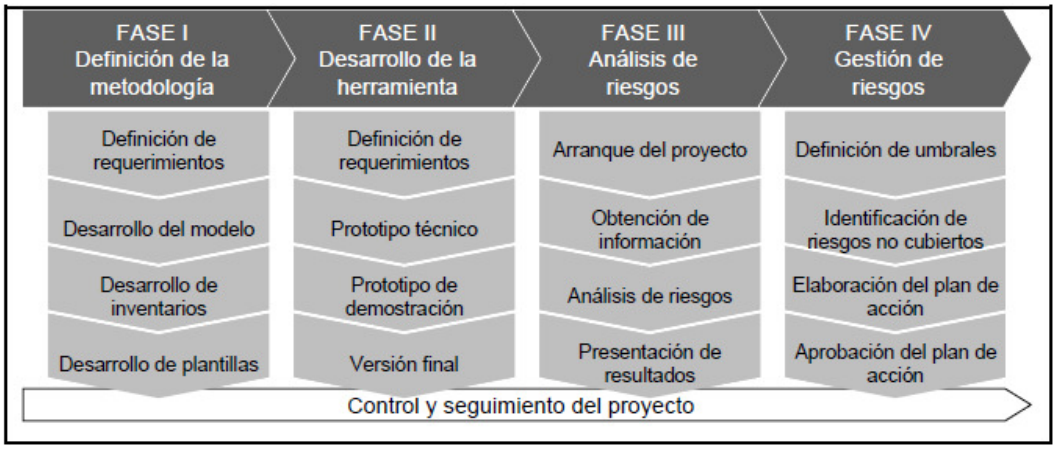


Figura 4. Fases del proyecto

En los siguientes apartados se encontraran más detalles cada una de las actividades vinculadas a las fases del TFM.

9.4 Metodología de análisis de riesgos:

Establece la sistemática que se seguirá para calcular el riesgo, lo cual deberá incluir básicamente la identificación y valoración de los activos, amenazas y vulnerabilidades. La definición de la metodología de análisis de riesgo la encontrar en el anexo Metodología de Análisis de Riesgos.

10. ANÁLISIS DE RIESGOS

IDENTIFICACIÓN DE LOS ACTIVOS

La identificación de los tipos de activos puede catalogarse como la información de tipo documental de todos aquellos elementos del sistema de información o relacionados con este, que generan un valor para el Tic Solution TIC SOLUTION, siendo necesarios para su buen funcionamiento y cumplimiento de los objetivos propuestos.

A continuación se clasifican los activos dentro de una estructura donde se determinará para cada uno de estos: el tipo de activo, el nombre y una breve descripción de las características, funciones y roles que cumplen para el Tic Solution.

Para ver la ficha de la identificación de activos (ver anexo 1).

[AUX] Equipamiento Auxiliar	
Se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.	
[AUX _ups] Sistemas de Alimentación Ininterrumpida	**(1)**
[AUX _gen] Generadores Eléctricos	**(2)**
[AUX _ac] Equipos de Climatización	**(3)**
[AUX _cabling] Cableado	**(4)**
[AUX _armario]armario archivador	**(5)**
1. Se cuenta con 2 UPS de energía regulada que es capaz de alimentar 16 equipos por 4 horas. 2. Se cuenta con 2 generadores eléctricos que son alimentados por 4 baterías de automotor 3. El Tic Solution 6 aires acondicionados de los cuales 2 son de tecnología mini split. 4. Entre la antena microondas y el switch acatel 6600 se utilizan enlaces de fibra y para el resto de la red se utiliza cable UTP categoría 5e Como medio de transmisión de datos para la interconexión entre equipos. 5. En estos se almacenan los documentos soportes impresos.	

[COM] Redes de Comunicaciones	
Es la infraestructura para que los datos se trasladen de un lugar a otro vía lógica.	
[COM_PSTN] Red Telefónica	**(1)**
[COM_radio] Red Inalámbrica	**(2)**
[COM_micro] Microondas	**(3)**
[COM_Red] Red	**(4)**

1. Es utilizada por el centro para la comunicación local, además para la comunicación con los distintos centros a larga distancia existe telefonía IP el servicio es proporcionado por Telecom.

2. Dentro del centro en los departamentos académicos existe una pequeña Lan inalámbrica que es soportada por un Access point y cuenta con una velocidad 10/100Mbits.

3. Existe una antena microondas que da conexión a los 3 centros que existen en bolívar y de las cuales una de ellas depende del Tic Solution que es centro náutico, esta conexión tiene un ancho para toda la regional Bolívar es de 1 Gigabyte, correspondiéndole a cada centro un canal de 341.33 Megabyte.

4. A nivel interno del centro se maneja una Lan que comunica todas las dependencias administrativas y académicas entre si, con una topología en estrella y 2 switch 3Com, 1 switch ACATEL, 1 switch NORTEL. A nivel de Red MAN utiliza el microondas para comunicarse con los otros centros que se encuentran en la ciudad de Cartagena.

[SI] Soporte de Información
Se consideran los dispositivos físicos que permiten almacenar información de forma permanente, o al menos durante largos periodos de tiempo
[Electronic] Electronicos **[CD]** Cd-Rom **(1)** **[usb]**Dispositivos USB **(2)** **[tape]** Cinta Magnética **(3)** **[Disk]** Discos Duros **(4)** **[Non_Electronic] No Electronicos** **[printed]** Material Impreso **(5)**
1. disco de almacenamiento con capacidad de 700 Mb de datos. 2. dispositivo de almacenamiento portable cuyas capacidad varia de 128 hasta 1GB. 3. disco magnético que se utiliza para sacar backup en el servidor donde está montada la aplicación de aportes. 4. dispositivos de almacenamiento que tiene un rango de 20GB a 80GB de marca Maxtor y Segate. 5. Contiene el material de respaldo sobre los datos y las diferentes operaciones que se manejan en el Tic Solution TIC SOLUTION.

[HW] Equipos Informáticos(Hardware)	
Son aquellos que sirven de herramienta para el almacenamiento, procesamiento y transporte de los datos lógicos y físicos en la empresa.	
[HW_S] servidores	**(1)**
[HW_PC] informática personal	**(2)**
[HW_PRINT] medios de impresión	**(3)**
[HW_switch] conmutadores	**(4)**
[HW_router] encaminadores	**(5)**
[HW_Cons] Consola de Descarga y video conferencia	**(6)**
[HW_Acces] Access point	**(7)**
[HW_Escan] Scanner	**(8)**
[HW _furniture] Mobiliario: Armarios, etc.	**(9)**

1. Servidor marca DELL de referencia Poweredge 6300 con capacidad de almacenamiento de 20Gb a 40Gb de disco y que se encuentra repartido en 6 disco, tiene 1 Ghz de memoria Ram, 2.4 Ghz en procesador, fuente de 650watt. Servidor marca IBM de serie 225(esta dañado) capacidad de almacenamiento de 80Gb de disco y que se encuentra repartido en 4 disco, tiene 1 Ghz de memoria Ram, 2.4 Ghz en procesador, fuente de 650watt.
2. Computadores personales se cuentan con 30 para la parte académica del centro y tiene de 40 a 80 Gb de disco duro de marca maxtor, 256 a 512 en memoria Ram, procesador Intel de 2.4 Ghz, una unidad de disquete, de Cd-ROM y 47 puertos usb.
3. Medios de impresión se tienen 10 con diferentes marcas y repartidas en todas las dependencias académicas.
4. Se cuenta en todo el centro con 4 switch con las siguientes referencias y características 1 switch acatel 6600 de 24 puertos con 4 puertos para fibra óptica, 2 switch 3Com de 24 puertos de series 3c16441a, fms2; 1

switch nortel de 24 puertos de la serie 24t70, 1 switch 3com de 12 puertos de serie fms2 todos los conmutadores mencionados tienen una velocidad de 10/100.

5. 1 router marca cisco.
6. Consola antivirus (PC dell de serie Gx 5200, 1 Ghz de ram, disco duro de 80 Gb, procesador 2.8 Ghz).
7. 1 accespoint cisco airones 1200 que da conectiva a las oficinas académicas.
8. 3 scanner para la digitalización de documentos.
9. Se cuentan con 2 armarios rack de 2 mts X 19'' en los cuales se encuentran los siguientes tipos de equipos: Switch, router, patch panel, modem de fibra.

[P] Personal	
Aparecen las personas relacionadas con los sistemas de información.	
[ui] Usuarios Internos	**(1)**
[P-Adm] Administradores de Sistemas	**(2)**
[P-Com] Administradores de Comunicaciones	**(3)**
[P-DBa] Administradores de Bases de Datos	**(4)**
[P-Desrr] Desarrolladores	**(5)**
[P_C_Acd] Coordinador académico	**(6)**
[P_SDir] Subdirector de Centro	**(7)**
[P_C_Pro] Coordinadora de formación profesional	**(8)**
[P_C_admin] Coordinador Administrativo	**(9)**
[P_C_TH] Talento Humano	**(10)**
[ue] Usuarios externos	**(11)**

1. Son aquellos que trabajan por mantener día a día la razón social de la empresa, como lo son los Trabajadores de planta, dentro de estos encontramos: registradora y certificadora, articulador e ingreso de alumnos, secretarias, aseadores, tutores y encargados del relacionamiento corporativo, compra y contratación.
2. Aquellas personas que organizan, administran, y dan soporte al sistema en general, el departamento de tecnología y sistemas.
3. Aquellas personas que organizan, administran, y dan soporte al sistema de comunicación y la infraestructura de red, el departamento de tecnología y sistemas.
4. La administración de la base de datos está a cargo del departamento de tecnología y sistemas.
5. El desarrollo actualización y sostenimiento de las páginas del Tic Solution está a cargo de grupo de tecnología y sistemas.
6. Se encarga de programar y gestionar todas las actividades de carácter académico dentro del Tic Solution.
7. gestiona y supervisa todos los procesos que se llevan a cabo en núcleo productivo.
8. Gestionar y apoyar los procesos que se llevan a cabo en la coordinación académica, articulación e ingreso de alumnos, relacionamiento corporativo y compras y contratación.
9. Gestiona todos los procesos relacionados con la parte administrativa de la empresa relacionada con cualquier transacción u operación financiera.
10. encargado de administrar los datos concernientes de la vida laboral de los empleados
11. Son personas que trabajan bajo un contrato establecido para prestar un servicio, en esta clasificación pueden entrar contratistas para mantenimiento de instalaciones físicas y equipos, profesores contratistas, como también los proveedores de servicios.

[SW] Aplicaciones (Software)
En esta clasificación se encuentran los activos con denominaciones concernientes a programas, aplicativos y desarrollos, para las tareas o procesos que han sido automatizadas en TIC SOLUTION. Su desempeño o utilización se realizaran a través de un equipo informático, en miras a gestionar, analizar y transformar los datos permitiendo la explotación de la información para la prestación de los servicios.
[prp] desarrollo propio **[SW_Fin2000]** Finanzas2000 **(1)** **[SW_Spem]** Servicio público de empleo **(2)** **[SW_Apl_web]** Pagina web del Tic Solution **(3)** **[SW_web_regi]** Pagina web de la regional Bolívar **(4)** **[sub]** desarrollo a medida (subcontratado) **[SW_SAGC]** sistema académico de gestión de centro **(5)** **[SW_SGVA]** sistema de gestión virtual de aprendices **(6)** **[SW_Adm2000]** Administración 2000 **(7)** **[SW_Cactus]** Biodata **(8)** **[SW_Tarant]**tarantela nomina **(9)** **[SW_Aport]** Aportes **(10)** **[std]** estándar **[SW_os]**sistemas operativos **(11)** **[SW_av]**antivirus **(12)** **[SW_Edpro]** Editores para el diseño y programación **(13)** **[SW_dbms]** sistemas de gestión de bases de datos **(14)** **[SW_lengpro]** lenguaje o plataforma de programación **(15)** **[SW_browser]** navegador web **(16)** **[Sw_email]** servicios de correo **(17)** **[Sw_office]** Ofimática **(18)**

1. Aplicación con la cual trabaja el departamento de contabilidad para registrar cualquier movimiento bancario o transacción. Este aplicativo corre en línea a través de la red MAN con la dirección general del **TIC SOLUTION** ubicada en la ciudad de Bogotá.

2. Plataforma web por medio de la cual el departamento de servicio público de empleo realiza la gestión, manejo y actualización de las hojas de vida, vacantes de empleo y las postulaciones de los usuarios ingresados en el sistema a esas vacantes. Igualmente se maneja la oferta de cursos a los cuales puede acceder los usuarios registrados en la plataforma.

3. Página web del **Tic Solution TIC SOLUTION** desarrollada bajo la tecnología php, java y flash en la cual se realizan publicaciones sobre las diferentes actividades de formación, culturales y pedagógicas del centro.

4. Página Web de la regional Bolívar **TIC SOLUTION** desarrollada bajo la tecnología php, java y flash en la cual se realizan publicaciones sobre las diferentes actividades de formación como la publicación de cursos y especialidades además soporte para desarrollar los cursos virtuales, por otra parte se presentan las diferentes actividades culturales y pedagógicas de la regional

5. Aplicación con la cual trabaja el departamento de coordinación académica y el Departamento de gestión de centros para manejar todo lo relacionado con la gestión de la oferta educativa tanto para las especialidades y cursos presénciales y virtuales. Este aplicativo corre en línea a través de la red MAN con la dirección general del **TIC SOLUTION** ubicada en la ciudad de Bogotá.

6. Aplicación con la cual trabaja el departamento de relacionamiento corporativo para la parte de oferta laboral y contratación de aprendices. Este aplicativo corre en línea a través de la red MAN con la dirección general del **TIC SOLUTION** ubicada en la ciudad de Bogotá.

7. Aplicación con la cual trabajan el departamento de Compras y Contratación y el departamento de Almacén e Inventarios. A través de esta aplicación se puede consultar la disponibilidad presupuestal y manejar los procedimientos a fines en cuanto a la parte de compra de equipos y contratación de instructores. Este aplicativo corre en línea a través de la red MAN con la dirección general del **TIC SOLUTION** ubicada en la ciudad de Bogotá.

8. Aplicación que se utiliza para llevar a cabo los procedimientos de seguridad social (prestaciones sociales, fondos y pensiones, subsidio de vivienda). Este aplicativo corre en línea a través de la red MAN con la dirección general del

TIC SOLUTION ubicada en la ciudad de Bogotá.

9. Aplicación utilizada para realizar todo los procedimientos de nómina específicamente en el manejo de datos concernientes y necesarios para la liquidación de la misma (horas de trabajo, salario, tipo de emolumento, legislaciones y normas). Este aplicativo corre en línea a través de la red MAN con la dirección general del **TIC SOLUTION** ubicada en la ciudad de Bogota.

10. Esta aplicación se utiliza para manejar y agilizar a través de la planilla única los aportes obligatorios que dan las empresas a las instituciones gubernamentales. Esta aplicación se encuentra corriendo a nivel local del Tic Solution, esta aplicación se encuentra instalada en el servidor IBM que posee el sistema operativo Windows 2000 Server que está ubicado en el dpto. de sistemas.

11. Se utiliza el sistema operativo Windows XP service pack 2 en todos los equipos informáticos que se encuentran en cada una de las oficinas y en los laboratorios informáticos, excepto en los servidor IBM que posee Windows 2000 Server y el servidor DELL que trabaja con Windows NT.

12. se cuenta con E-Trust Antivirus corporativo que está montado en todos los equipos del centro. Su actualización se realiza a través de una consola diariamente a las 5:00 PM.

13. se utiliza el paquete macromedia para la programación y diseño de la página. Este contiene las aplicaciones de flash, dreamweaver, firework, freehand entre otras.

14. Utilizan el motor MySql para la página web TIC SOLUTION http://Tic Solution.edu.co y Oracle para todas las aplicaciones que aparecen en los ítems 1, 2, 3, 4, 5, 6, 7, 8 y 9.

15. se utiliza el lenguaje de programación java con sus aplicaciones de java script y acción script para el diseño y desarrollo de la página web.

16. se utiliza Internet Explorer 6 y Mozilla como navegador web en todos los equipos del Tic Solution.

17. Para este fin se cuenta con el manejador de correspondencia Outlook y Microsoft Outlook con sus respectivos clientes. Además se cuenta con las respectivas cuentas de servicio correo de la dirección general llamado FTP.

18. Se cuenta con el paquete de office 2003 con todas sus herramientas.

[D] Datos / Información

[D_V]Datos Vitales.

[D_R_MIns]Reportes mensuales de instructores **(1)**

[D_P_Ofer]Plan de oferta educativa del centro **(2)**

[D_OyF] Oferta educativa y Formación ocupacional **(3)**

[D_E_Alum_C]Evaluaciones definitivas de alumnos participantes en cursos especiales. **(4)**

[D_E_Alum_M]Evaluaciones definitivas de alumnos por módulos o bloque modular. **(5)**

[D_L_Alum]Listado de alumnos aspirantes **(6)**

[D_L_Exa]Listado de examen **(7)**

[D_F_Eva]Formatos de evaluación de aprendizaje **(8)**

[D_J_R] Jóvenes rurales e institutos **(9)**

[D_C] Datos Clasificados.

[D_R] reservado **(10)**

[D_C] confidencial **(11)**

[D_SC] datos sin clasificar **(12)**

[D_C] Datos de carácter personal

[D_Apr]Información sobre aprendices TIC SOLUTION **(13)**

[D_Ins_p]Dato**s** instructores. **(14)**

[D_P_plan]Datos del personal de planta. **(15)**

[D_com] Datos de interés comercial

[D_Com]Órdenes de compra	**(16)**
[D_Cot]listado de cotizaciones	**(17)**
[D_Pres]Solicitud presupuestal	**(18)**

1. Los reportes mensuales de instructores contienen todo sobre las actividades académicas de las especialidades presénciales y cursos para iniciar el proceso de certificación.

2. Estos contienen los datos concernientes al proceso de elección de las especialidades para los nuevos periodos académicos.

3. En estos se encuentran los datos de las especialidades, cursos presénciales y virtuales, el tutor asignado, intensidad horaria, estructura curricular a los que pueden acceder e inscribirse el público.

4. Estos datos contiene la nota final de los aprendices que están realizando cursos en convenio entre una institución, población civil y el TIC SOLUTION.

5. Son las notas de los aprendices que se encuentran vinculados al TIC SOLUTION estudiando una especialidad técnica o tecnológica por demanda social.

6. Se encuentra la lista de los alumnos aspirantes a una especialidad y alcanzaron todos los logros y méritos para un cupo dentro de la especialidad.

7. Contiene la evaluación que se le realizara a los aspirantes a una especialidad dentro del Tic Solution.

8. Estos contiene las pautas que debe tener el tutor para evaluar a los aprendices y los aprendices al tutor (guías de aprendizaje).

9. Contiene los datos sobre las poblaciones especiales (ubicación, tipo de población) y los programas que se van a llevar acabo en ellas, además cuenta con los programas de formación que se llevan a cabo en las

instituciones e institutos.

10. Las contraseñas de servidores, licencia del software, Backup y contraseñas personales, Datos De Administración De Página Web, código fuente de la página Web, Consultas a Bases De Datos, datos de nómina, prestaciones sociales.

11. En estos datos encontramos Manuales de registro de alumnos, Manuales de ingreso de alumnos, procesos de contratación de los instructores.

12. Se encuentra el cronograma de mantenimiento y aseo, actividades de carácter informativo sobre eventos y actividades de formación en el centro, como también comunicados a los estudiantes e instructores y el listado de las la Empresas y su respectiva cuota de patrocinio de estudiantes Tic Solution.

13. Se tienen los datos personales de los alumnos del Tic Solution, contrato con alguna empresa patrocinadora, especialidad, número de orden, ficha social y seguro contra accidente.

14. Aquí se encuentra los datos personales de los tutores y sus respectivos contratos con el Tic Solution, los módulos que dictan e intensidad horaria.

15. Aquí se encuentra los datos personales y sus respectivos contratos con el Tic Solution (Horario de trabajo, tipo de vinculación, emolumentos etc.).

16. Tienen todos los datos concernientes para la realizar la compra de un artículo o bien, e igualmente la contratación de algún servicio.

17. estos contienen las cotizaciones que se necesitan para hacer un estudio para la compra de un equipo. Por lo general se manejan 3 de cotizaciones de proveedores diferentes.

18. información que contiene los fondos monetarios disponibles con los cuales cuenta el centro para la adquisición, compra y mantenimiento de un equipo y planta.

[S] Servicios
Los activos de tipo servicio con los que cuenta el Tic Solution TIC SOLUTION pueden definirse como aquellos activos que con su Función o ejecución pueden satisfacer una necesidad de los usuarios (clientes que utilizan el servicio) tanto a usuarios internos como externos. Dentro de los tipos de servicios podemos encontrar. ✓ **Servicios a usuarios Internos:** Son aquellos servicios que se prestan a entre los departamentos o usuarios internos dentro del mismo Tic Solution. ✓ **Servicios al Público:** Son aquellos servicios que presta el *TIC SOLUTION Tic Solution* al público en general, a instituciones u organizaciones. ✓ **Servicios Contratados:** Son los servicios que prestan otras organizaciones como los Outsourcing y contratistas, que se son necesarios para que el *Tic Solution TIC SOLUTION* pueda realizar a cabo ciertos procesos o procedimientos de manera exitosa.
[pub] Servicios al publico en general **[S_Capacit]** Servicio de capacitación y formación **(1)** **[S_Aten]** Atención a la demanda educativa **(2)** **[S_Recorp]** Relacionamiento Corporativo **(3)** **[S_InforWeb]** Información en el portal Web **(4)** **[ext] Servicios Internos** **[S_C_cont]** compras y contratación **(5)**

[S_C_Acad] Servicio de coordinación académica	**(6)**
[S_C_ForP] Coordinación De Formación Profesional	**(7)**
[S_RegC] Registro y Certificación de alumnos	**(8)**
[S_Adm_R_BD]Administración de red y base de datos	**(9)**
[S_soport]Soporte técnico	**(10)**
[S_Di_web]Diseño y administración de página web	**(11)**
[S_DHCP] Asignación de direcciones dinámicas	**(12)**
[S_ Ftp] Transferencia de archivos	**(13)**
[S_ LiqNom] Liquidación de nómina	**(14)**
[cont] Servicios Contratado a Terceros	
[S_Mant_p_e] Servicio de mantenimiento de planta y equipos	**(15)**
[S_Inst] Instructores contratistas	**(16)**
[S_Internet] Internet	**(17)**

1. Servicio que se presta a la población Colombia que requiera formación y certificación tecnológica y técnica profesional de manera virtual o presencial.

2. Maneja todo lo relacionado con la atención de la demanda educativa, esto incluye los procesos de información de cursos, módulos y especialidades abiertas, inscripción e ingreso de alumnos.

3. Atención a la demanda de las empresas de sector público y privado que necesiten aprendices TIC SOLUTION para realizar la etapa productiva en sus instalaciones (prácticas o pasantías empresariales).

4. información sobre las actividades y eventos de carácter cultural, académicos y productivos del Tic Solution.

5. servicio encargado de la contratación del personal del mantenimiento de planta y equipos (equipamiento auxiliar e informático) e instructores contratistas. También se maneja todo lo pertinente a la compra de

maquinarias, equipos e insumos.

6. Se encarga de programar y gestionar todas las actividades de carácter académico dentro del Tic Solution.

7. Gestionar y apoyar los procesos que se llevan a cabo en la coordinación académica, articulación e ingreso de alumnos, relacionamiento corporativo y compras y contratación.

8. Se encarga del registro de estudiantes con sus respectivas notas al sistema, y la entrega de los certificados de los cursos culminados.

9. Monitorea el funcionamiento de la red interna e igualmente realiza soporte técnico para el manejo y administración de la página Web de la regional Bolívar www.Tic Solution.edu.co , aplicaciones en línea y bases de datos.

10. Soporte técnico para el funcionamiento de equipos informáticos.

11. Desarrollo, diseño, administración y mantenimiento de la Pagina Web http://Tic Solution.edu del Tic Solution.

12. Servicio encargado de la asignación dinámica de direcciones IP.

13. Servicio encargado de la transferencia electrónica de archivos entre las regionales del TIC SOLUTION.

14. Servicio de liquidación de nómina, afiliación a la salud, pensión, ARP, capacitación y bienestar del personal de planta del Tic Solution bolívar.

15. Servicio contratado por el Tic Solution a empresas particulares para el mantenimiento de planta e instalaciones y equipamiento auxiliar. Para el mantenimiento de equipos informáticos se contacta a la empresa DELL y a COMPUSISCA.

16. Instructores contratados por el Tic Solution para dictar los módulos de formación.

17. Para el servicio de Internet se contrató al proveedor TELECOM.

DIAGRAMAS DE DEPENDENCIA DE LOS ACTIVOS

A continuación se realiza la relación de los diagramas de dependencias que nos permitirán identificar que activos de la organización de orden superior dependen de los activos de orden inferior para así que nos sirva de insumo para el análisis de riesgo.

DIAGRAMA DEL SERVIDOR

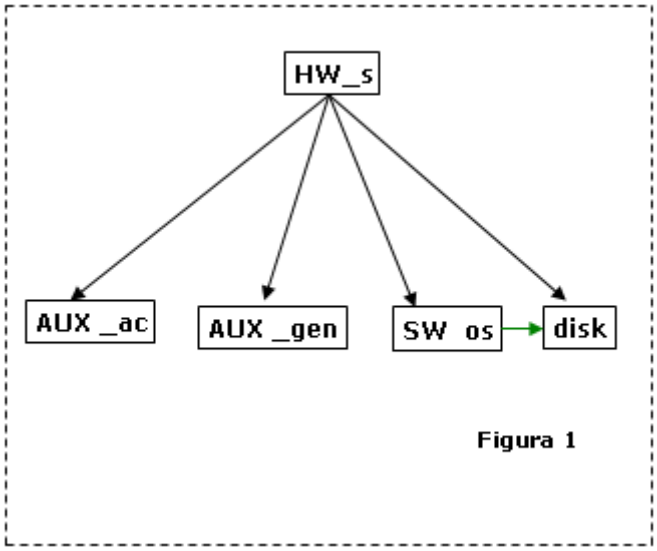


Figura 1

UPS

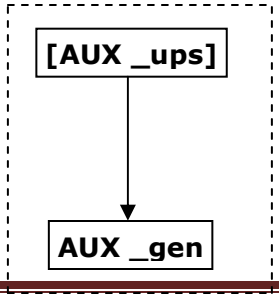


DIAGRAMA DE RED

RED LAN

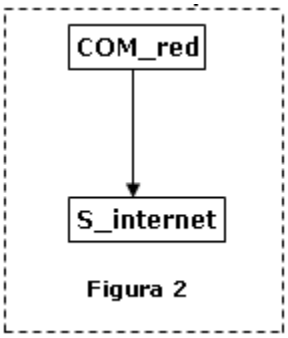


Figura 2

RED WAN Y MAN

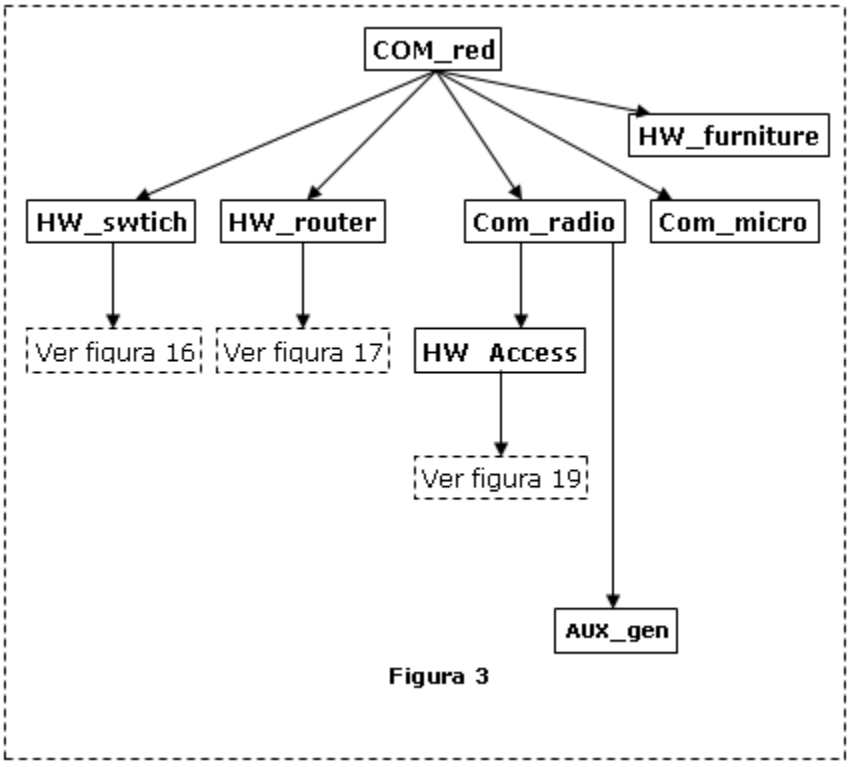


Figura 3

DIAGRAMA DE LA APLICACIÓN WEB DEL TIC SOLUTION

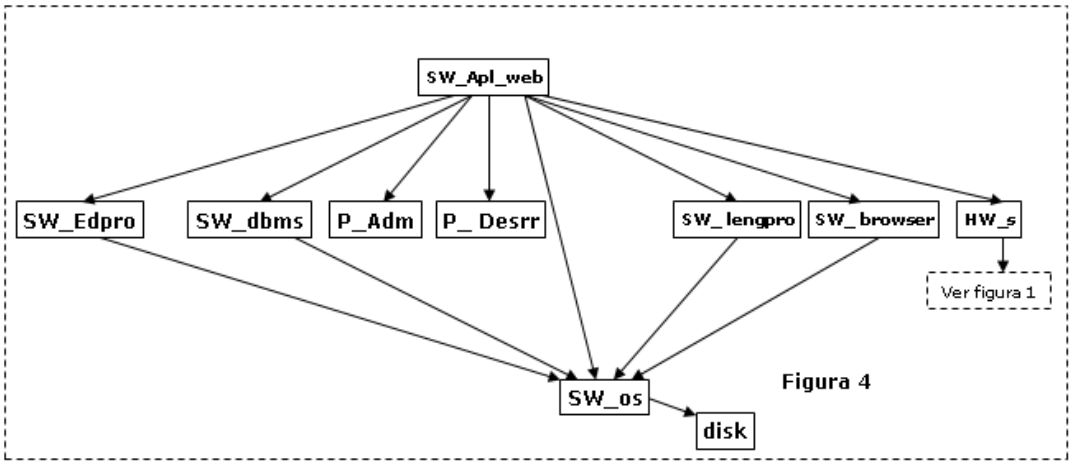


Figura 4

DIAGRAMA DE LA APLICACIÓN WEB DE LA REGIONAL BOLÍVAR

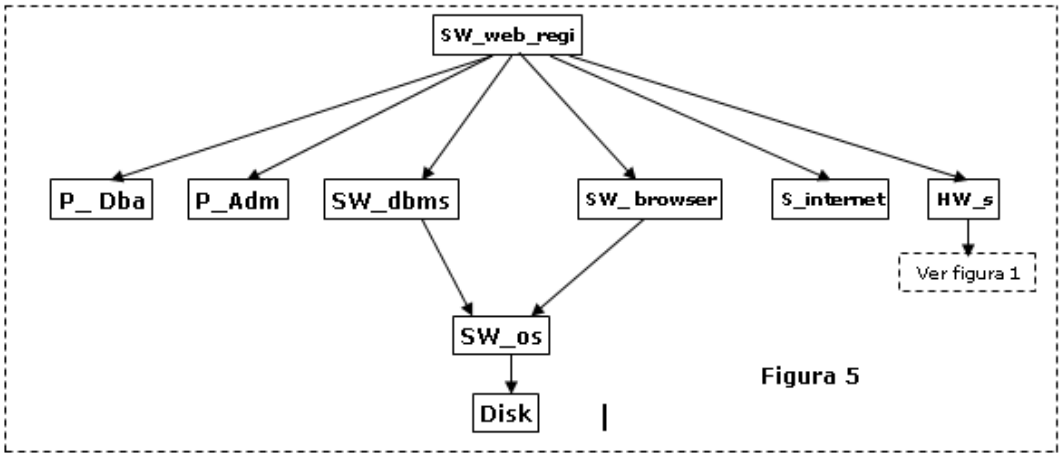


Figura 5

DIAGRAMA DE LA APLICACIÓN WEB DEL SERVICIO PUBLICO DE EMPLEO

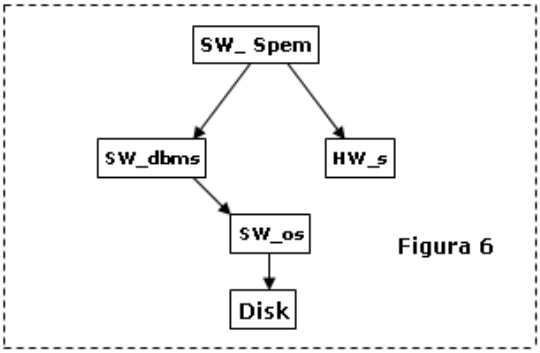


Figura 6

DIAGRAMA SISTEMA DE GESTIÓN VIRTUAL DE APRENDICES

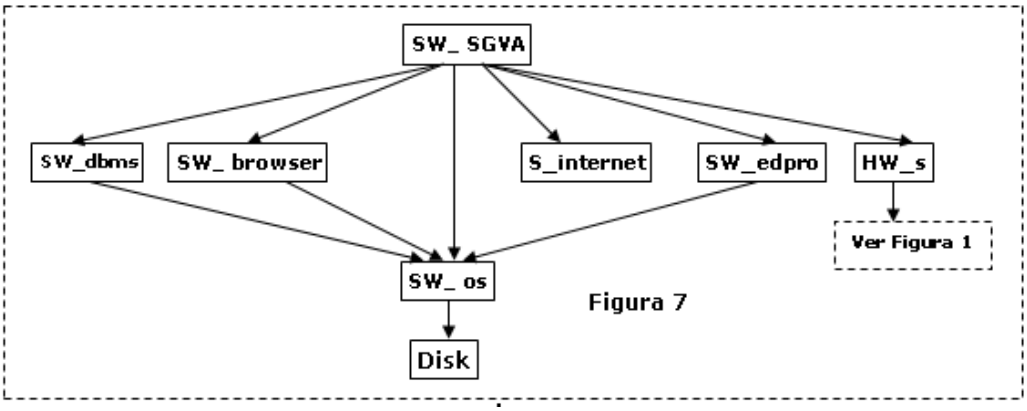


Figura 7

DIAGRAMA SISTEMA ACADÉMICO DE GESTIÓN DE CENTRO

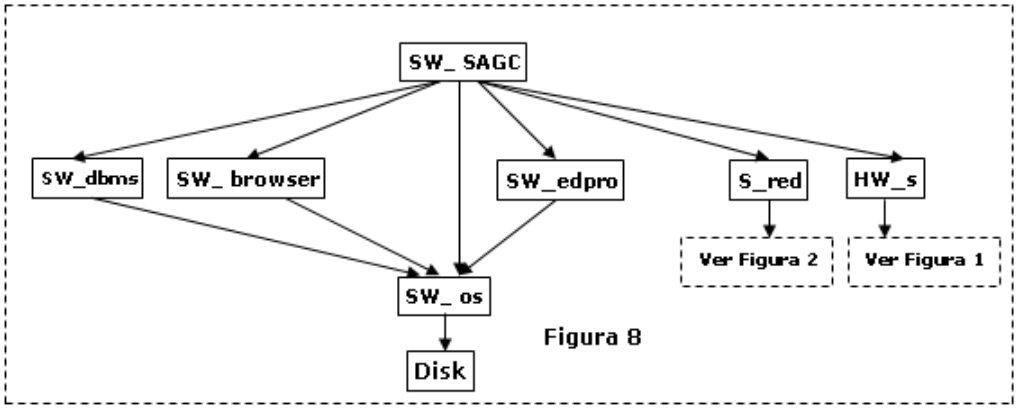


Figura 8

DIAGRAMA DE LA APLICACIÓN FINANZAS 2000

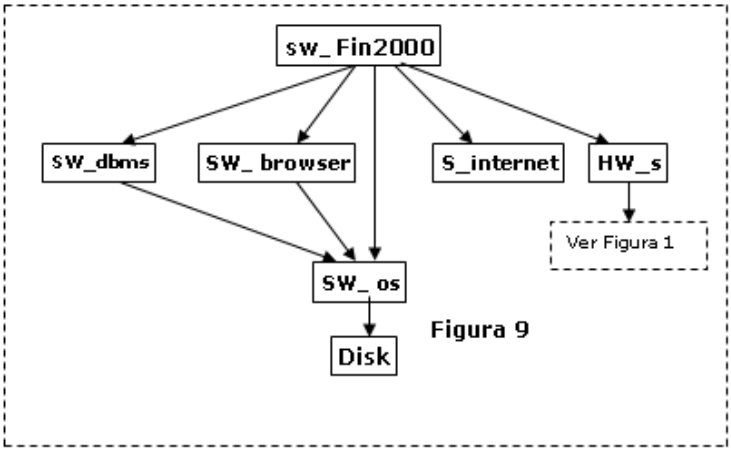


Figura 9

DIAGRAMA DE LA APLICACIÓN ADMINISTRACIÓN 2000

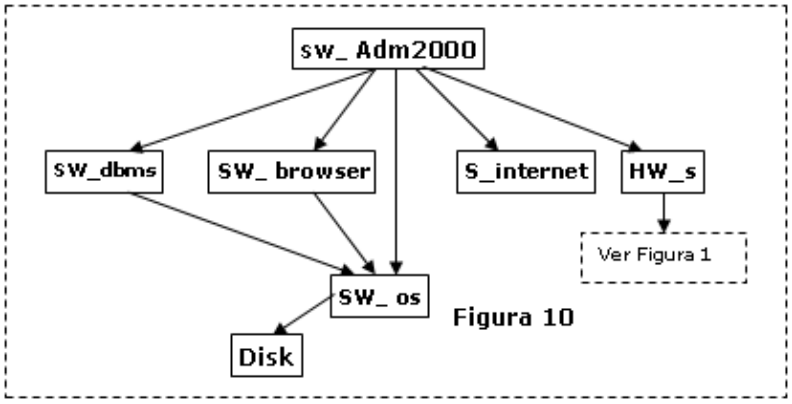


Figura 10

DIAGRAMA DE LA APLICACIÓN CAPTUS BIODATA

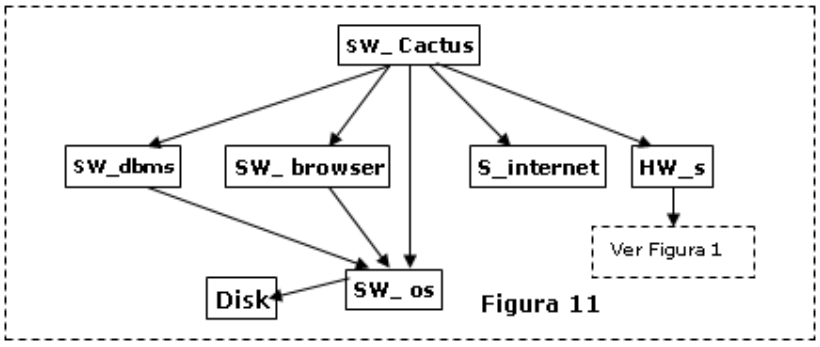


Figura 11

DIAGRAMA DE LA APLICACIÓN TARANTELA NOMINA

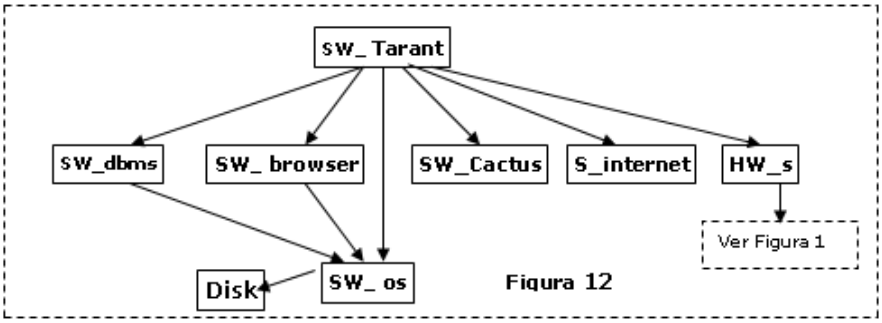


DIAGRAMA DE LA APLICACIÓN APORTES

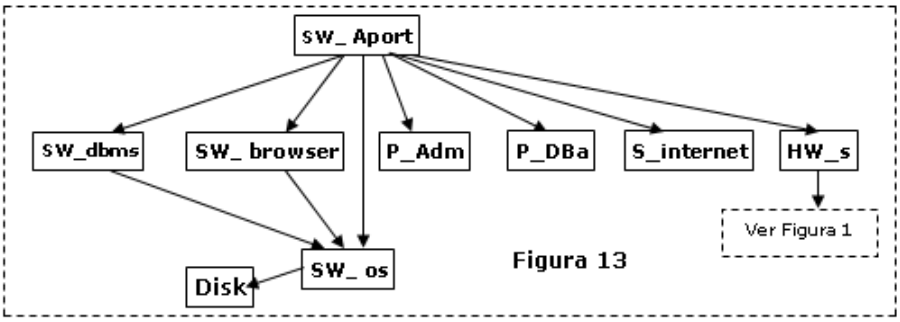


DIAGRAMA COMPUTADOR PERSONAL

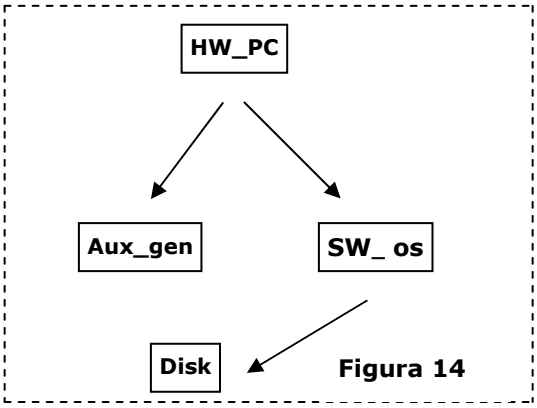


Figura 14

DIAGRAMA IMPRESORA

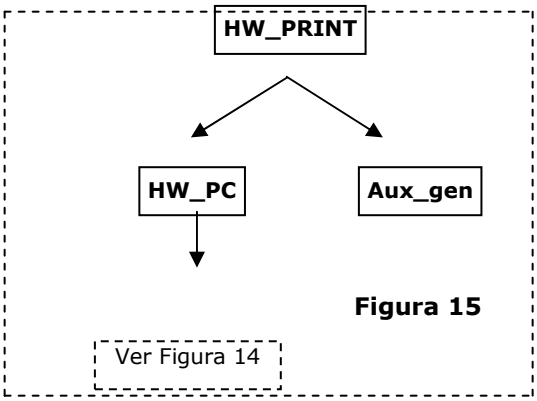


Figura 15

DIAGRAMA SWITCH

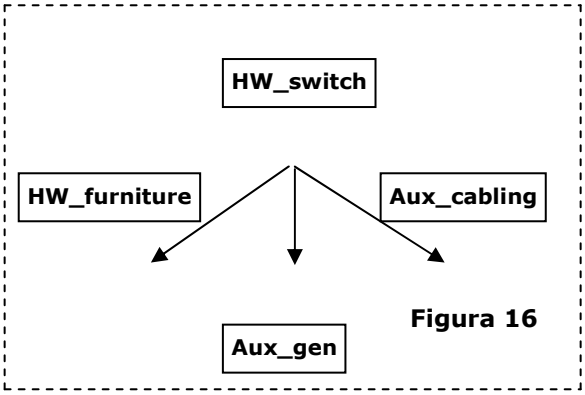


Figura 16

DIAGRAMA ROUTER

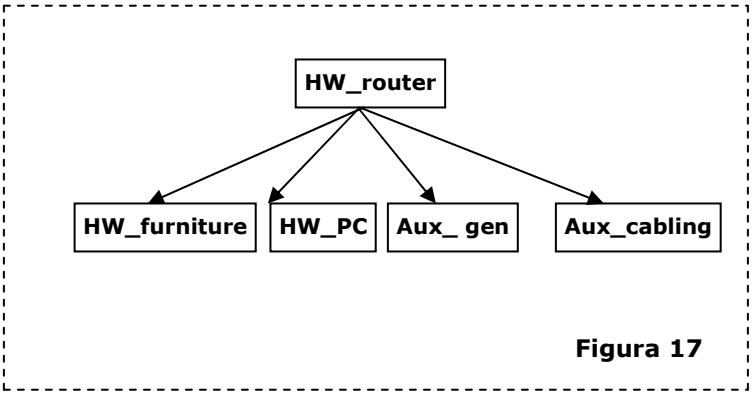


Figura 17

DIAGRAMA DE CONSOLA DE DESCARGA

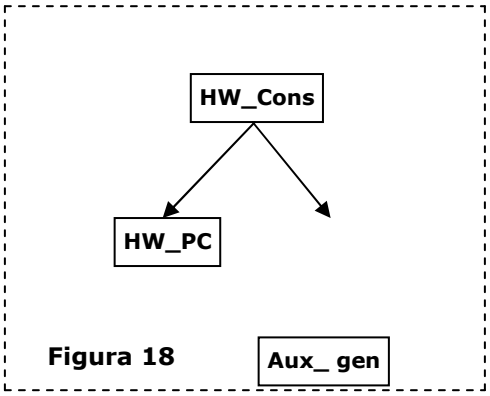


Figura 18

DIAGRAMA ACCESS POINT

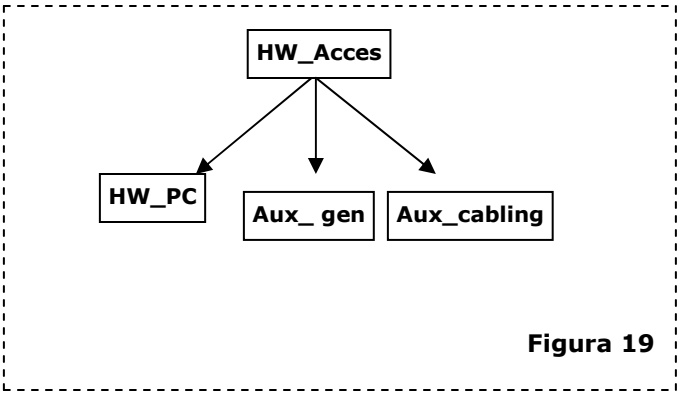


Figura 19

DIAGRAMA DE ESCÁNER

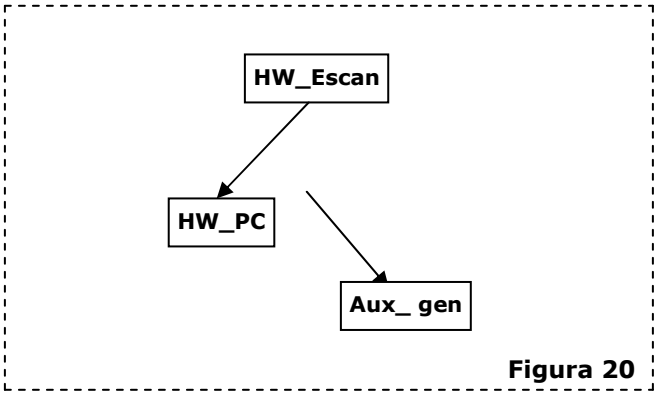


Figura 20

DIAGRAMA DE EMAIL

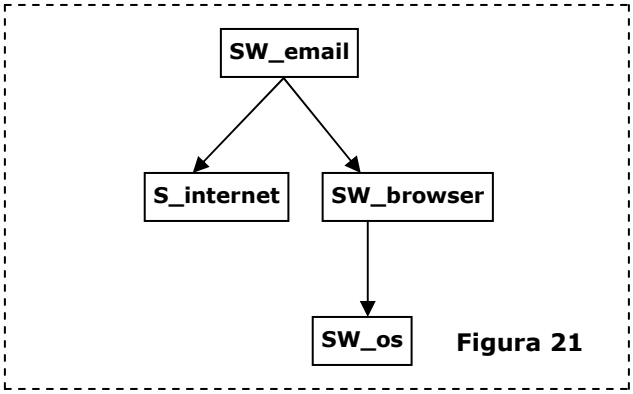


Figura 21

DIAGRAMA DE MATERIAL IMPRESO

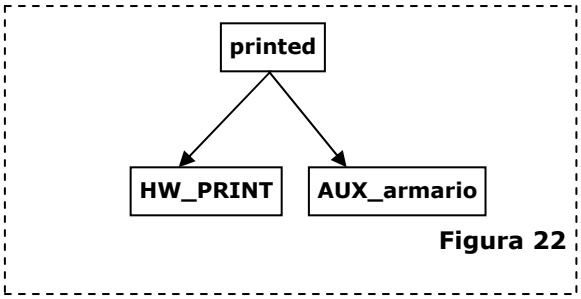


Figura 22

DIAGRAMA SERVICIO FTP

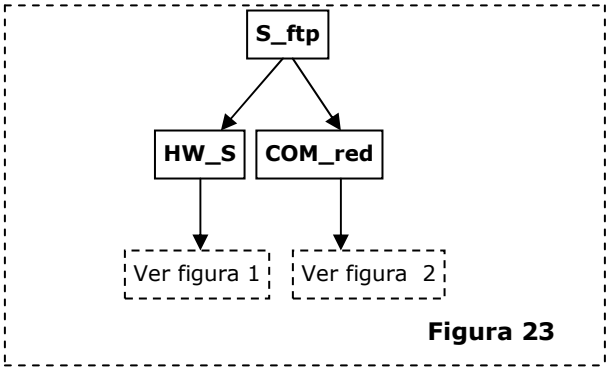


Figura 23

DIAGRAMA DATOS OFERTA EDUCATIVA Y FORMACIÓN OCUPACIONAL

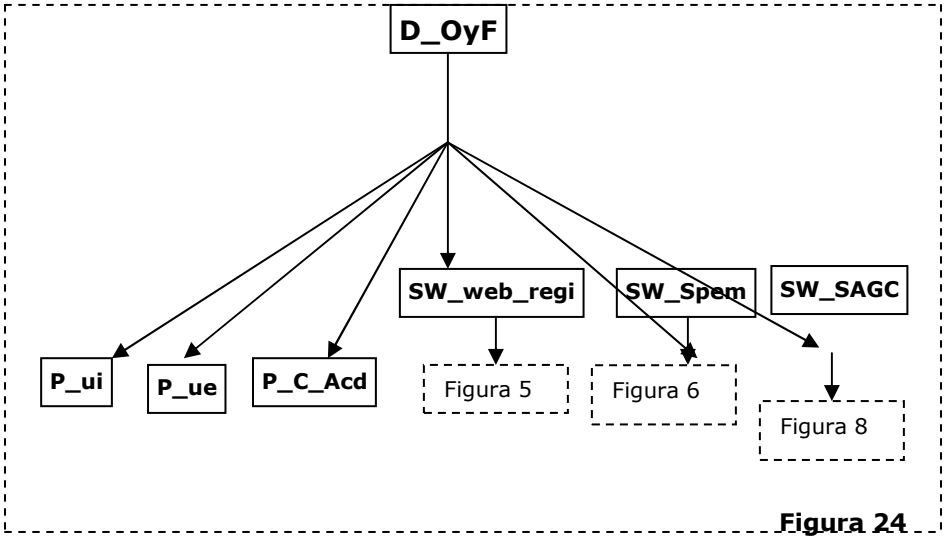


Figura 24

DIAGRAMA DATOS EVALUACIONES DEFINITIVAS DE ALUMNOS

PARTICIPANTES EN CURSOS ESPECIALES

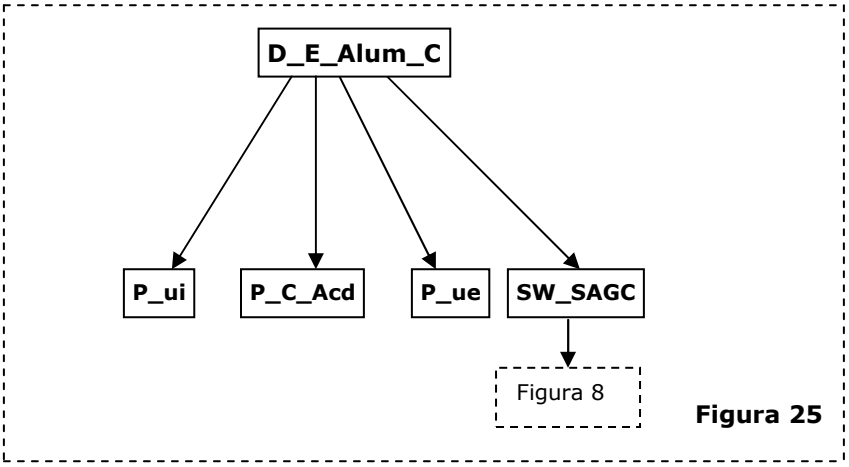


Figura 25

DIAGRAMA DATOS EVALUACIONES DEFINITIVAS DE ALUMNOS

POR MÓDULOS O BLOQUE MODULAR

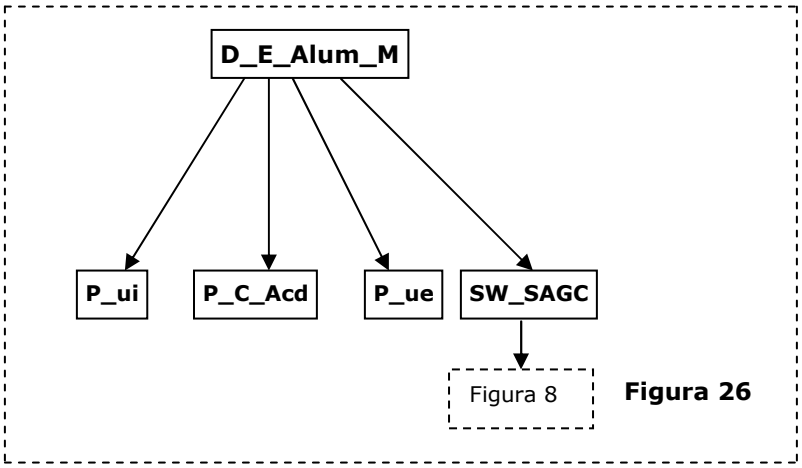


Figura 26

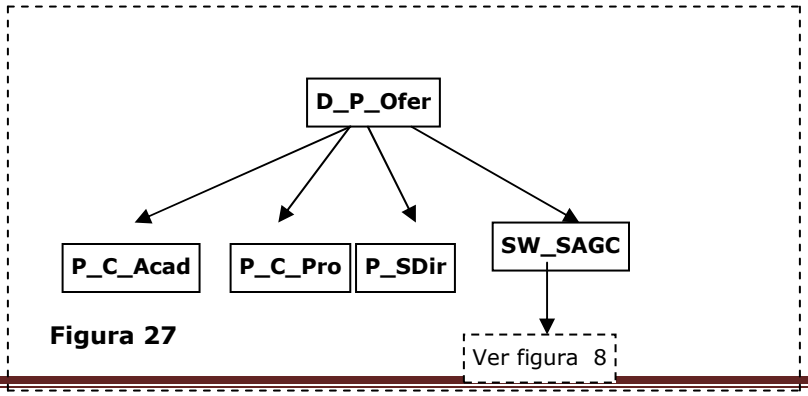


Figura 27

DIAGRAMA DATOS PLAN DE OFERTA EDUCATIVA

DIAGRAMA DATOS RESERVADOS

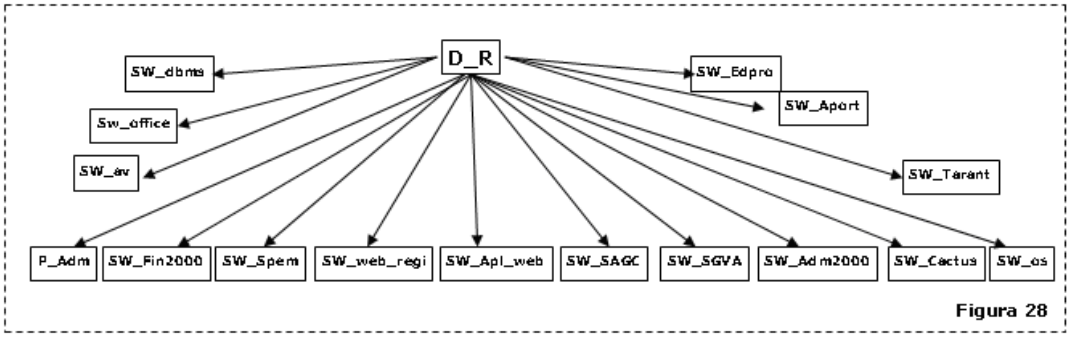


Figura 28

DIAGRAMA DATOS FORMATOS DE EVALUACIÓN DE APRENDIZAJE

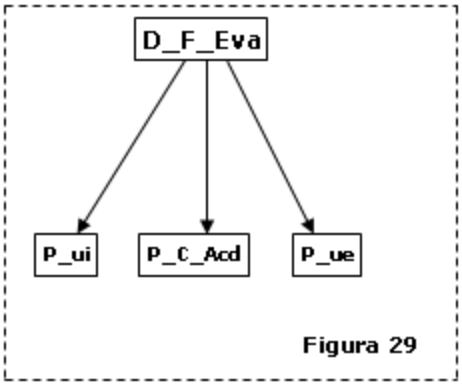


Figura 29

DIAGRAMA DATOS CONFIDENCIAL

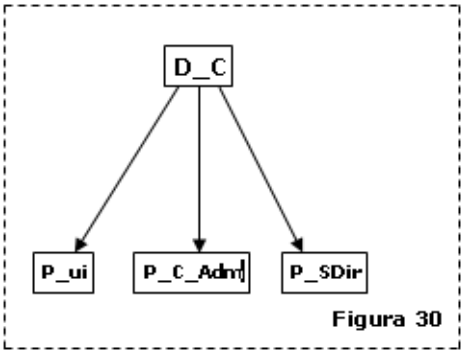


Figura 30

DIAGRAMA DATOS SIN CLASIFICAR

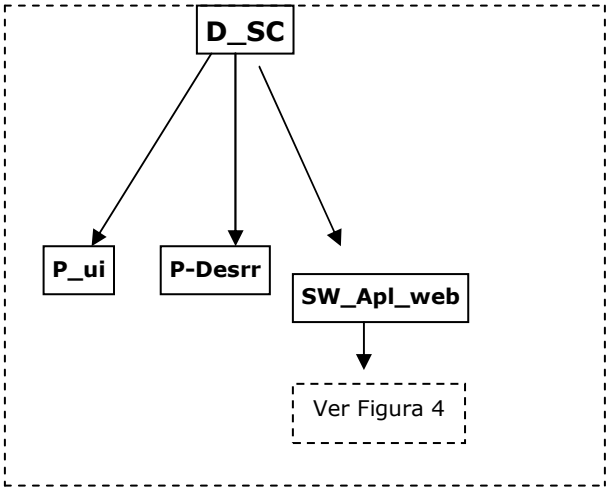


DIAGRAMA RED TELEFÓNICA

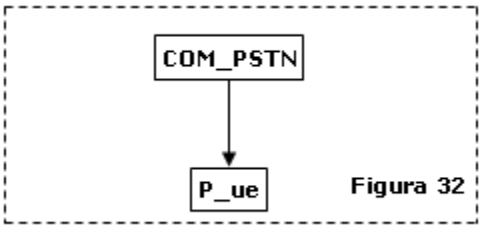


DIAGRAMA SERVICIO DE CAPACITACIÓN

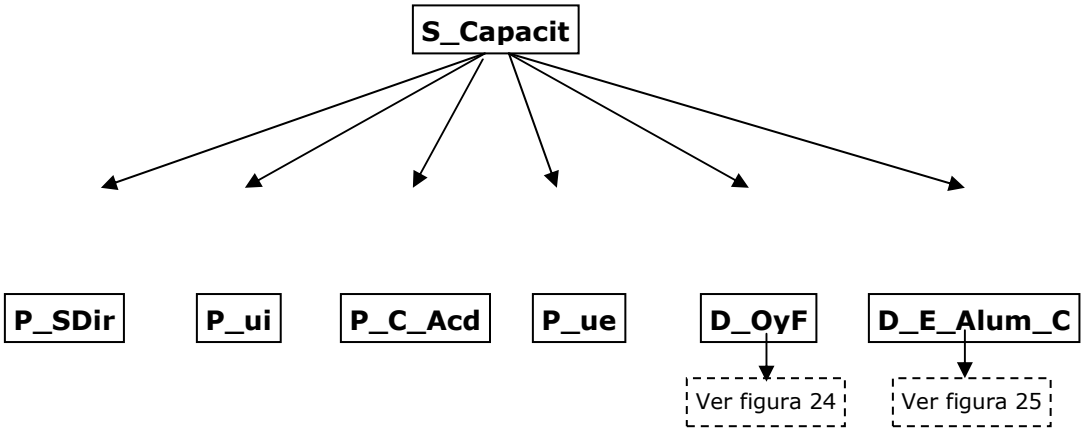


DIAGRAMA SERVICIO DE ATENCIÓN A LA DEMANDA EDUCATIVA

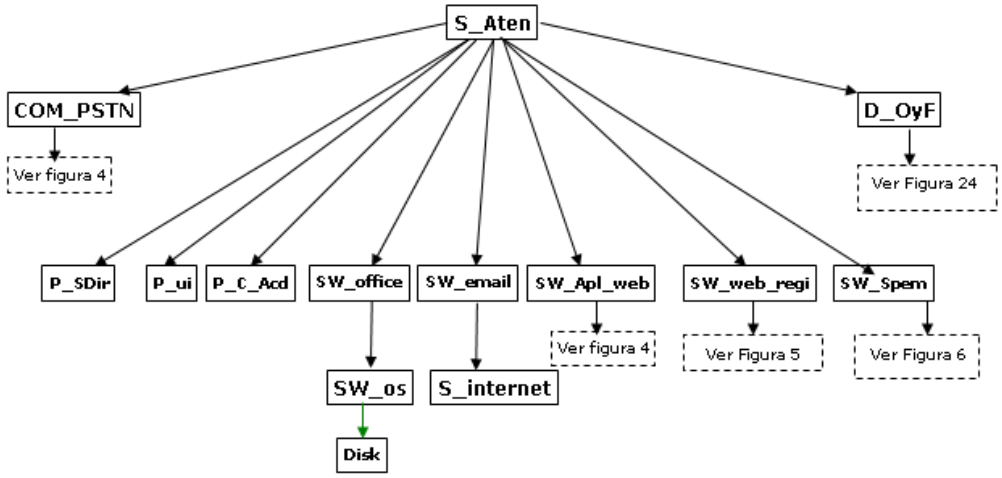


DIAGRAMA SERVICIO DE RELACIONAMIENTO CORPORATIVO

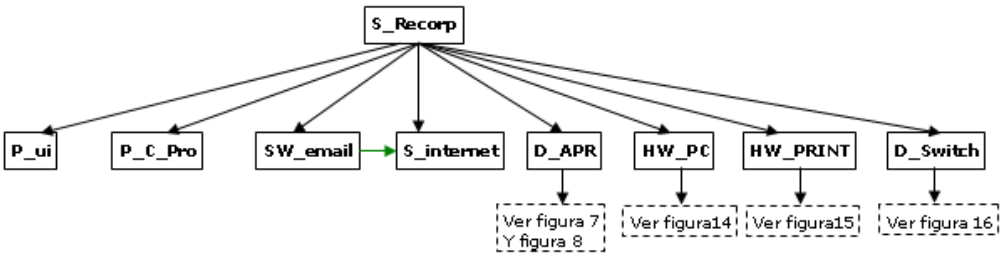


DIAGRAMA SERVICIO INFORMACIÓN EN EL PORTAL WEB

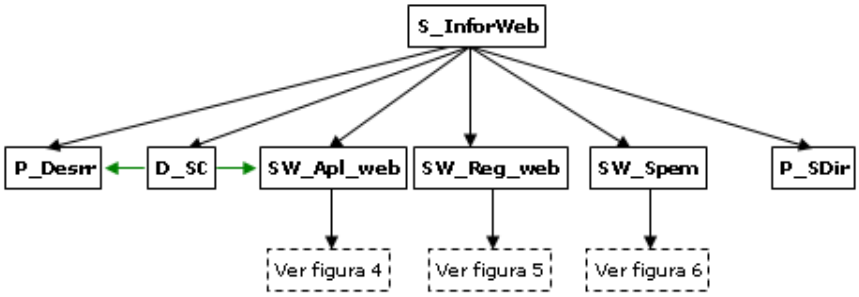


DIAGRAMA SERVICIO COMPRAS Y CONTRATACIÓN

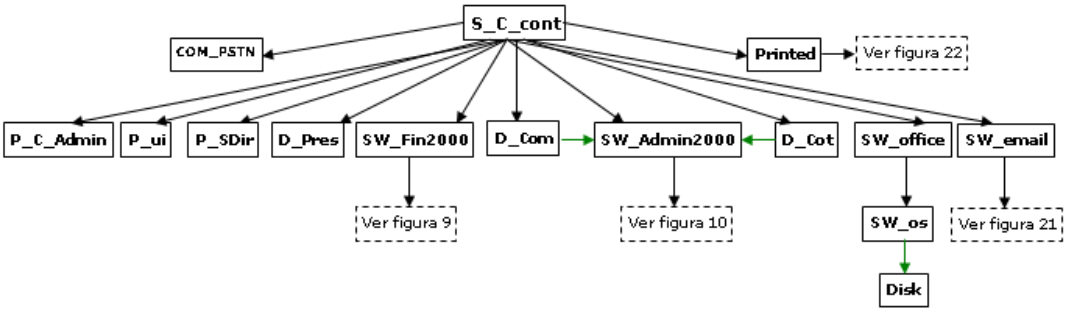


DIAGRAMA SERVICIO COORDINACIÓN ACADÉMICA

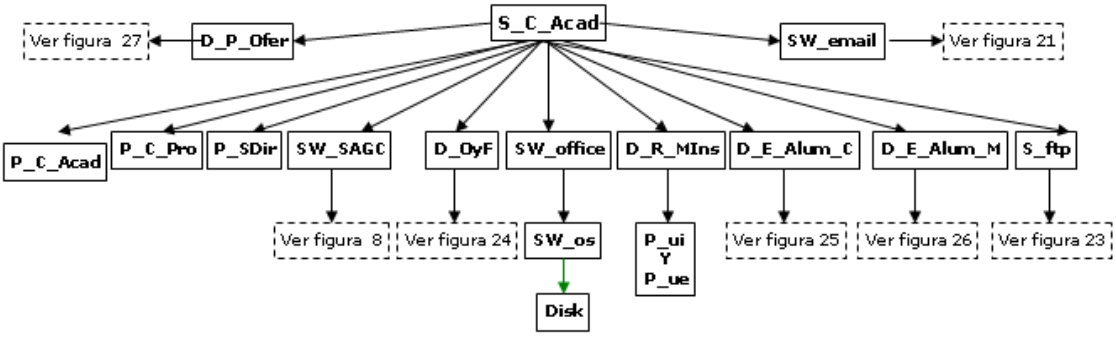


DIAGRAMA SERVICIO COORDINACIÓN DE FORMACIÓN PROFESIONAL

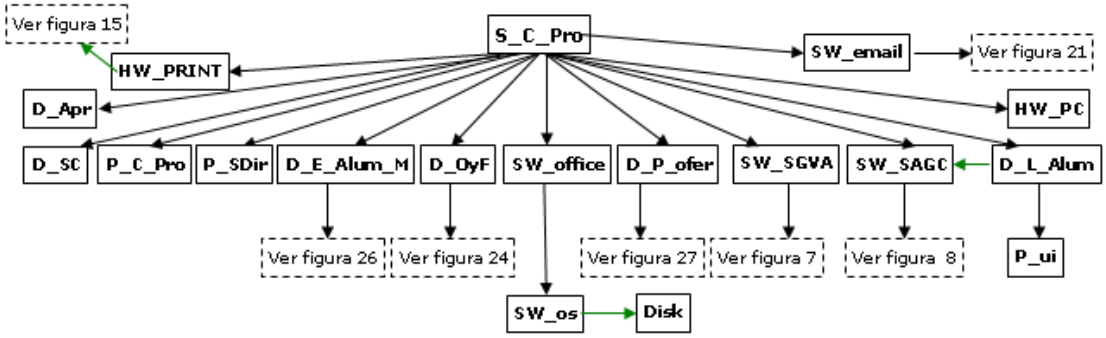


DIAGRAMA SERVICIO REGISTRO Y CERTIFICACIÓN

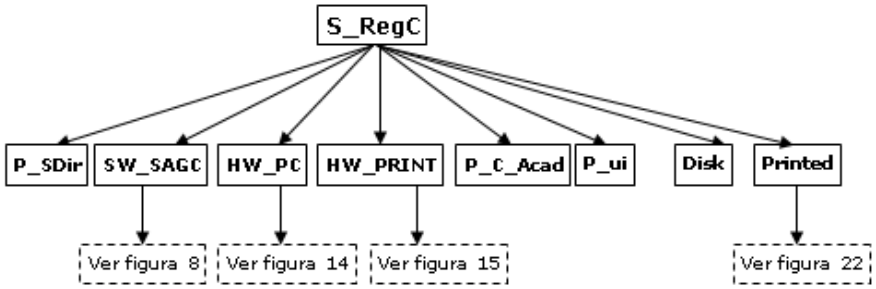


DIAGRAMA SERVICIO ADMINISTRACIÓN DE RED Y BASE DE DATOS

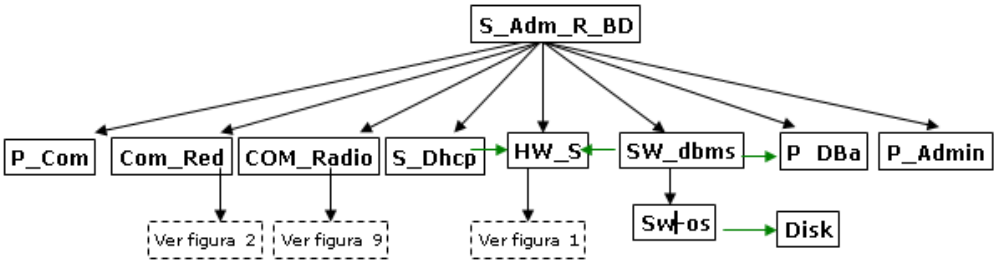


DIAGRAMA SOPORTE TÉCNICO

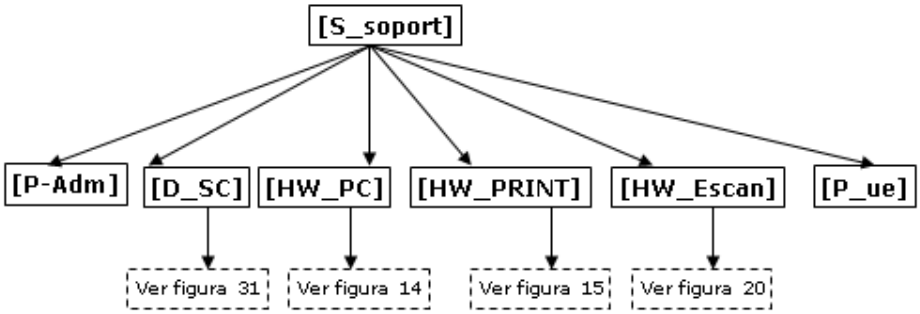


DIAGRAMA DE SERVICIO DE DISEÑO Y ADMINISTRACIÓN DE PAGINA WEB

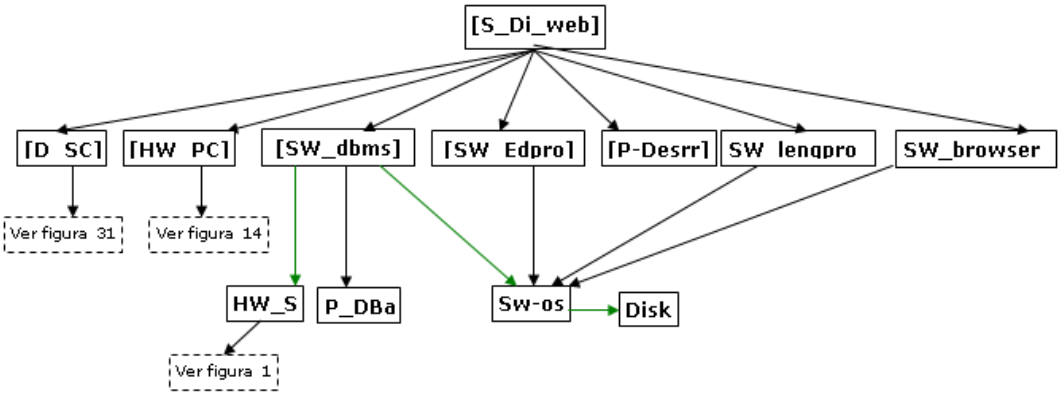


DIAGRAMA SERVICIO DE ASIGNACIÓN DE DIRECCIONES DINÁMICAS (DHCP)

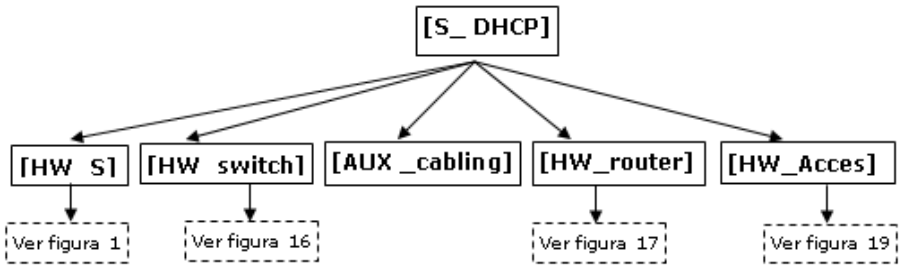


DIAGRAMA SERVICIO DE LIQUIDACIÓN DE NOMINA

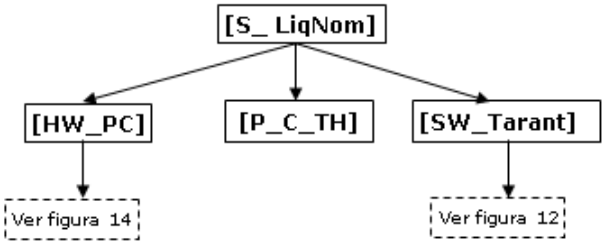


DIAGRAMA SERVICIO DE MANTENIMIENTO DE PLANTA Y EQUIPOS

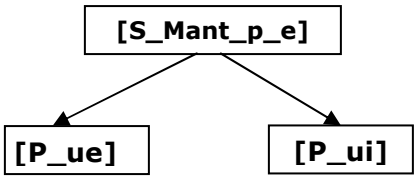


DIAGRAMA SERVICIO DE INSTRUCTORES CONTRATISTAS

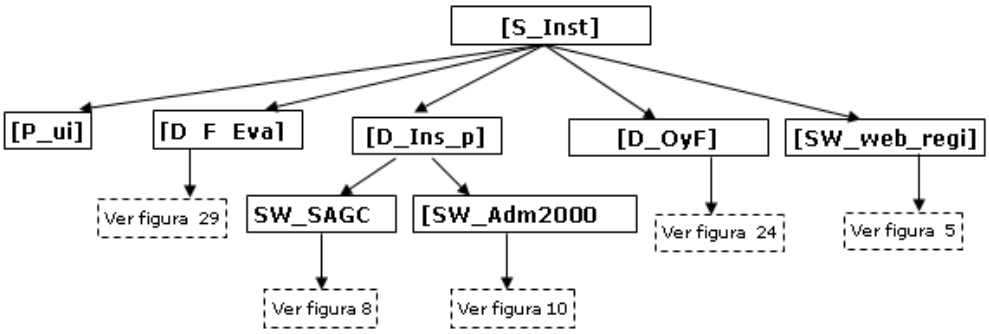


DIAGRAMA SERVICIO DE INTERNET

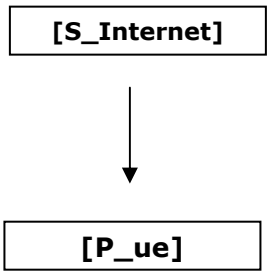


DIAGRAMA DE APLICACIÓN ANTIVIRUS

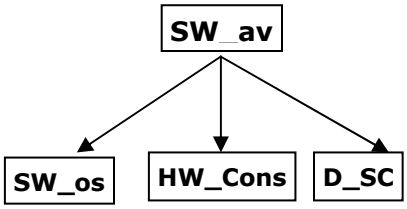


DIAGRAMA DATOS JÓVENES RURALES E INSTITUTOS

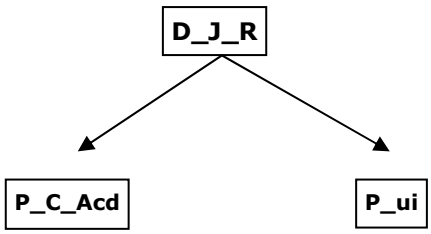
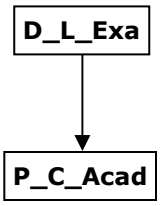


DIAGRAMA DATOS DE LISTADO DE EXAMEN



TABLAS DE DEPENDENCIA

A continuación se realiza la relación de las tablas de dependencias que nos permitirán tener una imagen global de la dependencia de un activo en relación con todos los activos identificados en la institución.

	[P_ui]	[P-Adm]	[P-Com]	[P-DBa]	[P-Desrr]	[P_C_Acd]	[P_SDir]	[P_C_Pro]	[P_C_admin]	[P_C_TH]	[P_ue]	[SW_Fin2000]	[SW_Spem]	[SW_web_regi]	[SW_Apl_web]	[SW_SAGC]	[SW_SGVA]	[SW_Adm2000]	[SW_Cactus]	[SW_Tarant]	[SW_Aport]	[SW_os]	[SW_av]	[SW_Edpro]	[SW_dbms]
[P_ui]																									
[P-Adm]																									
[P-Com]																									
[P-DBa]																									
[P-Desrr]																									
[P_C_Acd]																									
[P_SDir]																									
[P_C_Pro]																									
[P_C_admin]																									
[P_C_TH]																									
[P_ue]																									
[SW_Fin2000]																						√			√
[Sw_email]																									
[Sw_office]																						√			
[SW_Spem]																						√			√
[SW_Apl_web]		√			√																	√		√	√
[SW_SAGC]																						√			√
[SW_web_regi]		√		√																		√			√
[SW_SGVA]																						√		√	√
[SW_Adm2000]																						√			√
[SW_Cactus]																						√			√
[SW_Tarant]																			√			√			√
[SW_Aport]		√		√																		√			√
[SW_os]																									
[SW_av]																						√			
[SW_Edpro]																						√			
[SW_dbms]				√																		√			
[SW_lengpro]																						√			
[SW_browser]																						√			
[S_Capacit]	√					√	√				√														
[S_Aten]	√					√	√						√	√	√										
[S_Recorp]	√							√									√								
[S_InforWeb]					√		√						√	√	√										
[S_C_cont]	√						√		√			√						√							
[S_C_Acad]						√	√	√								√									
[S_C_ForP]							√	√								√	√								
[S_ReqC]	√					√	√									√									
[S_Adm_R_BD]		√	√	√																					√
[S_soport]		√									√														
[S_Di_web]					√																			√	√
[S_DHCP]																									
[S_Ftp]																									
[S_LigNom										√										√					

	[Sw_email]	[Sw_office	[SW_lengpro]	[SW_browser]	[S_Capacit]	[S_Aten]	[S_Recorp]	[S_InforWeb]	[S_C_cont]	[S_C_Acad]	[S_C_ForP]	[S_RegC]	[S_Adm_R_ BD]	[S_soport]	[S_Di_web]	[S_DHCP]	[S_ Ftp]	[S_ LiqNom [S_Mant_p_e]	[S_Inst]	[S_Internet]	[D_R_MIns]	[D_P_Ofer]	[D_OyF]	[D_E_Alum_C]	[D_E_Alum_M]	[D_L_Alum]
[P_ui]																										
[P-Adm]																										
[P-Com]																										
[P-DBa]																										
[P-Desrr]																										
[P_C_Acd]																										
[P_SDir]																										
[P_C_Pro]																										
[P_C_admin]																										
[P_C_TH]																										
[P_ue]																										
[Sw_email]				√																√						
[Sw_office]																										
[SW_Fin2000]				√																√						
[SW_Spem]																										
[SW_Apl_web]			√	√																						
[SW_web_regi]				√																√						
[SW_SAGC]				√																√						
[SW_SGVA]				√																√						
[SW_Adm2000]				√																√						
[SW_Cactus]				√																√						
[SW_Tarant]				√																√						
[SW_Aport]				√																√						
[SW_os]																										
[SW_av]																										
[SW_Edpro]																										
[SW_dbms]																										
[SW_lengpro]																										
[SW_browser]																										
[S_Capacit]																							√			√
[S_Aten]	√	√																					√			
[S_Recorp]	√																			√						
[S_InforWeb]																										
[S_C_cont]	√	√																								
[S_C_Acad]	√	√															√				√	√	√	√	√	
[S_C_ForP]	√	√																				√	√		√	√
[S_RegC]																										
[S_Adm_R_ BD]																√										
[S_soport]																										
[S_Di_web]			√	√																						
[S_DHCP]																										
[S_ Ftp]																										
[S_ LiqNom																										

	[D_J_Exa]	[D_E_Eva]	[D_J_R]	[D_R]	[D_C]	[D_SC]	[D_Apr]	[D_Ins_p]	[D_P_plan]	[D_Com]	[D_Cot]	[D_Pres]	[HW_S]	[HW_PC]	[HW_PRINT]	[HW_switch]	[HW_router]	[HW_Cons]	[HW_Acces]	[HW_Escan]	[HW_furniture]	[AUX _ups]	[AUX _gen]	[AUX _ac]
[P_ui]																								
[P-Adm]																								
[P-Com]																								
[P-DBa]																								
[P-Desrr]																								
[P_C_Acd]																								
[P_SDir]																								
[P_C_Pro]																								
[P_C_admin]																								
[P_C_TH]																								
[P_ue]																								
[Sw_email]																								
[Sw_office]																								
[SW_Fin2000]													√											
[SW_Spem]													√											
[SW_Apl_web]						√							√											
[SW_web_regi]													√											
[SW_SAGC]													√											
[SW_SGVA]													√											
[SW_Adm2000]													√											
[SW_Cactus]													√											
[SW_Tarant]													√											
[SW_Aport]													√											
[SW_os]																								
[SW_av]						√												√						
[SW_Edpro]																								
[SW_dbms]													√											
[SW_lengpro]																								
[SW_browser]																								
[S_Capacit]																								
[S_Aten]																								
[S_Recorp]							√							√	√	√								
[S_InforWeb]						√							√											
[S_C_cont]										√	√	√												
[S_C_Acad]						√	√	√							√									
[S_C_ForP]						√	√							√	√									
[S_RegC]														√	√									
[S_Adm_R_ BD]													√											
[S_soport]						√								√	√					√				
[S_Di_web]						√								√										
[S_DHCP]													√			√	√		√					
[S_ Ftp]													√											
[S_ LigNom														√										

	[AUX _cabling]	[AUX _armario]	[COM_PSTN]	[COM_radio]	[COM_micro]	[COM_Red]	[COM_Internet]	[CD]	[usb]	[tape]	[Disk]	[printed]
[P_ui]												
[P-Adm]												
[P-Com]												
[P-DBa]												
[P-Desrr]												
[P_C_Acd]												
[P_SDir]												
[P_C_Pro]												
[P_C_admin]												
[P_C_TH]												
[P_ue]												
[Sw_email]												
[Sw_office]												
[SW_Fin2000]												
[SW_Spem]												
[SW_Apl_web]												
[SW_web_regi]												
[SW_SAGC]												
[SW_SGVA]												
[SW_Adm2000]												
[SW_Cactus]												
[SW_Tarant]												
[SW_Aport]												
[SW_os]											√	
[SW_av]												
[SW_Edpro]												
[SW_dbms]												
[SW_lengpro]												
[SW_browser]												
[S_Capacit]												
[S_Aten]			√									
[S_Recorp]			√			√	√	√	√		√	√
[S_InforWeb]							√				√	
[S_C_cont]			√									√
[S_C_Acad]			√	√							√	√
[S_C_ForP]			√	√								√
[S_RegC]											√	√
[S_Adm_R_ BD]				√		√	√					
[S_soport]												
[S_Di_web]												
[S_DHCP]	√											
[S_ Ftp]						√						
[S_ LinNom												

	[P_ui]	[P-Adm]	[P-Com]	[P-DBa]	[P-Desrr]	[P_C_Acd]	[P_SDir]	[P_C_Pro]	[P_C_admin]	[P_C_TH]	[P_ue]	[SW_Fin2000]	[SW_Spem]	[SW_web_regi]	[SW_Apl_web]	[SW_SAGC]	[SW_SGVA]	[SW_Adm2000]	[SW_Cactus]	[SW_Tarant]	[SW_Aport]	[SW_os]	[SW_av]	[SW_Edpro]	[SW_dbms]
[S_Mant_p_e]	√										√														
[S_Inst]	√													√											
[S_Internet]											√														
[D_R_MIns]	√										√														
[D_P_Ofer]						√	√	√								√									
[D_OyF]	√					√					√		√	√		√									
[D_E_Alum_C]	√					√					√					√									
[D_E_Alum_M]	√					√					√					√									
[D_L_Alum]	√															√									
[D_L_Exa]						√																			
[D_F_Eva]	√					√					√														
[D_J_R]	√					√																			
[D_R]		√										√	√	√	√	√	√	√	√	√	√	√	√	√	√
[D_C]	√	√					√																		
[D_SC]	√				√										√										
[D_Apr]																√	√								
[D_Ins_p]																√				√					
[D_P_plan]																			√	√					
[D_Com]																		√							
[D_Cot]																		√							
[D_Pres]												√													
[HW_S]																						√			
[HW_PC]																						√			
[HW_PRINT]																									
[HW_switch]																									
[HW_router]																									
[HW_Cons]																									
[HW_Acces]																									
[HW_Escan]																									
[HW_furniture]																									
[AUX_ups]																									
[AUX_gen]																									
[AUX_ac]																									
[AUX_cabling]																									
[AUX_armario]																									
[COM_PSTN]																									
[COM_radio]																									
[COM_micro]																									
[COM_Red]																									
[COM_Internet]																									
[CD]																									
[usb]																									
[tape]																									
[Disk]																									

	[Sw_email]	[Sw_office]	[SW_lengpro]	[SW_browser]	[S_Capacit]	[S_Aten]	[S_Recorp]	[S_InforWeb]	[S_C_cont]	[S_C_Acad]	[S_C_ForP]	[S_RegC]	[S_Adm_R_BD]	[S_soport]	[S_Di_web]	[S_DHCP]	[S_LigNom. [S_Fip]	[S_Mant_p_e]	[S_Inst]	[S_Internet]	[D_R_MIns]	[D_P_Ofer]	[D_OyF]	[D_E_Alum_C]	[D_E_Alum_M]	[D_L_Alum]
[S_Mant_p_e]																										
[S_Inst]																							√			
[S_Internet]																										
[D_R_MIns]																										
[D_P_Ofer]																										
[D_OyF]																										
[D_E_Alum_C]																										
[D_E_Alum_M]																										
[D_L_Alum]																										
[D_L_Exa]																										
[D_E_Eva]																										
[D_J_R]																										
[D_R]		√																								
[D_C]																										
[D_SC]																										
[D_Apr]																										
[D_Ins_p]																										
[D_P_plan]																										
[D_Com]																										
[D_Cot]																										
[D_Pres]																										
[HW_S]																										
[HW_PC]																										
[HW_PRINT]																										
[HW_switch]																										
[HW_router]																										
[HW_Cons]																										
[HW_Acces]																										
[HW_Escan]																										
[HW_furniture]																										
[AUX_ups]																										
[AUX_gen]																										
[AUX_ac]																										
[AUX_cabling]																										
[AUX_armario]																										
[COM_PSTN]																										
[COM_radio]																										
[COM_micro]																										
[COM_Red]																										
[COM_Internet]																										
[CD]																										
[usb]																										
[tape]																										
[Disk]																										
[printed]																										

	[D_L_Exa]	[D_F_Eva]	[D_J_R]	[D_R]	[D_C]	[D_SC]	[D_Apr]	[D_Ins_p]	[D_P_plan]	[D_Com]	[D_Cot]	[D_Pres]	[HW_S]	[HW_PC]	[HW_PRINT]	[HW_switch]	[HW_router]	[HW_Cons]	[HW_Acces]	[HW_Escan]	[HW_furniture]	[AUX_ups]	[AUX_gen]	[AUX_ac]
[S_Mant_p_e]																								
[S_Inst]		√						√																
[S_Internet]																								
[D_R_MIns]																								
[D_P_Ofer]																								
[D_OyF]																								
[D_E_Alum_C]																								
[D_E_Alum_M]																								
[D_L_Alum]																								
[D_L_Exa]																								
[D_F_Eva]																								
[D_J_R]																								
[D_R]																								
[D_C]																								
[D_SC]																								
[D_Apr]																								
[D_Ins_p]																								
[D_P_plan]																								
[D_Com]																								
[D_Cot]																								
[D_Pres]																								
[HW_S]																							√	√
[HW_PC]																							√	
[HW_PRINT]														√									√	
[HW_switch]																				√			√	
[HW_router]														√						√			√	
[HW_Cons]														√									√	
[HW_Acces]														√									√	
[HW_Escan]														√									√	
[HW_furniture]																								
[AUX_ups]																							√	
[AUX_gen]																								
[AUX_ac]																							√	
[AUX_cabling]																								
[AUX_armario]																								
[COM_PSTN]																								
[COM_radio]																			√				√	
[COM_micro]																							√	
[COM_Red]																√	√		√		√		√	
[COM_Internet]																								
[CD]																								
[usb]																								
[tape]																								
[Disk]																								
[printed]															√									

VALORIZACIÓN DE LOS ACTIVOS

Son las características o atributos que hacen valioso un activo. Estos se valoran por medio de dimensiones o facetas lo cual conlleva a que la valoración que recibe un activo en cierta dimensión es la medida del perjuicio del activo.

A continuación se explican cada una de las dimensiones de valoración para los activos.

[D] 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 para el Tic Solution TIC SOLUTION?
✓ Un activo tiene un gran valor desde el punto de vista de disponibilidad si una amenaza afectara a su disponibilidad, las consecuencias serían graves. ✓ 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.

[I] 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. ✓ los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna.

[C] 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. ✓ Los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

[A_S] 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. ✓ un servicio recibe una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para el Tic Solution TIC SOLUTION. ✓ un servicio carece de un valor apreciable desde el punto de vista de autenticidad cuando su acceso por cualquiera no supone preocupación alguna.

[A_D] 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. ✓ Los datos carecen de un valor apreciable desde el punto de vista de autenticidad del origen cuando ignorar la fuente es irrelevante.

VALORACIÓN

	Dimensión de valoración de seguridad			
ACTIVO	**[D]**	**[I]**	**[C]**	**[A]**
[S_Capacit] Servicio de capacitación y formación	**[10][1]**			**[1][3]**
[S_Aten] Atención a la demanda educativa	**[10][1]**			**[2][1]**
[S_Recorp] Relacionamiento Corporativo	**[3][2]**			**[1][8]**
[S_InforWeb] Información en el portal Web	**[1][8]**			**[0][4]**
[S_C_cont] compras y contratación	**[7][5]**			**[9][6.2]**
[S_C_Acad] Servicio de coordinación académica	**[10][1]**			**[5][1]**
[S_C_ForP] Coordinación De Formación Profesional	**[4][1]**			**[2][1]**
[S_RegC] Registro y Certificación de alumnos	**[9][1]**			**[6][3]**

[S_Adm_R_BD]Administración de red y base de datos	**[9]**[1]			**[9]**[5]
[S_soport]Soporte técnico	**[7]**[1]			**[1]**[1]
[S_Di_web]Diseño y administración de página web	**[1]**[5]			**[1]**[5]
[S_DHCP] Asignación de direcciones dinámicas	**[5]**[2]			**[3]**[10]
[S_ Ftp] Transferencia de archivos	**[5]**[2]			**[4]**[1]
[S_ LiqNom] Liquidación de nomina	**[7]**[1]			**[3]**[6.3]
[S_Mant_p_e] Servicio de mantenimiento de planta y equipos	**[7]**[1]			**[1]**[1]
[S_Inst] Instructores contratistas	**[7]**[4]			**[5]**[4]
[S_Internet] Internet	**[10]**[2]			**[7]**[2]
[D_R_MIns]Reportes mensuales de instructores		**[9]**[1]	**[6]**[5]	**[4]**[2]
[D_P_Ofer]Plan de oferta educativa del centro		**[10]**[1]	**[9]**[12]	**[9]**[7]
[D_OyF] Oferta educativa y Formación ocupacional		**[9]**[1]	**[1]**[3]	**[9]**[4]
[D_E_Alum_C]Evaluaciones definitivas de alumnos Participantes en cursos especiales.		**[4]**[3]	**[6]**[5]	**[7]**[11]
[D_E_Alum_M]Evaluaciones definitivas de alumnos por módulos o bloque modular.		**[4]**[3]	**[6]**[5]	**[7]**[11]
[D_L_Alum]Listado de alumnos aspirantes		**[6]**[3]	**[0]**[1]	**[5]**[3.2]
[D_L_Exa]Listado de examen		**[5]**[1]	**[7]**[11]	**[1]**[1]
[D_F_Eva]Formatos de evaluación de aprendizaje		**[6]**[3]	**[7]**[11]	**[6]**[1]

[D_J_R] Jóvenes rurales e institutos		**[9]**[1]	**[6]** [5]	**[1]**[1]
[D_R] reservado		**[10]**[3]	**[7]**[8]	**[10]**[3]
[D_C] confidencial		**[3]**[2]	**[9]**[1]	**[5]**[1]
[D_SC] datos sin clasificar		**[5]**[10]	**[5]**[10]	**[5]**[10]
[D_Apr]Información sobre aprendices TIC SOLUTION		**[6]**[1]	**[6]**[5]	**[3]**[7]
[D_Ins_p]Datos instructores.		**[6]**[2]	**[6]**[2]	**[5]**[10]
[D_P_plan]Datos del personal de planta.		**[6]**[2]	**[6]**[2]	**[5]**[10]
[D_Com]Órdenes de compra		**[7]**[6.3]	**[7]**[6.2]	**[7]**[6.3]
[D_Cot]Listado de cotizaciones		**[7]**[6.4]	**[7]**[7]	**[7]**[6.3]
[D_Pres]Solicitud presupuestal		**[7]**[6.3]	**[7]**[6.3]	**[7]**[6.3]
[SW_Fin2000] Finanzas2000	**[7]**[4]	**[7]**[6.3]	**[3]**[6.2]	**[9]**[8]
[SW_Spem] Servicio público de empleo	**[9]**[1]	**[9]**[4]	**[9]**[5]	**[6]**[1]
[SW_Apl_web] Pagina web del Tic Solution	**[1]**[5]	**[9]**[1]	**[0]**[2]	**[6]**[1]
[SW_web_regi] Pagina web de la regional Bolívar	**[9]**[1]	**[9]**[1]	**[0]**[2]	**[9]**[1]
[SW_SAGC] sistema académico de gestión de centro	**[10]**[2]	**[9]**[4]	**[9]**[5]	**[9]**[8]
[SW_SGVA] sistema de gestión virtual de aprendices	**[9]**[5]	**[5]**[7]	**[4]**[1]	**[4]**[1]
[SW_Adm2000] Administración 2000	**[7]**[4]	**[7]**[6.3]	**[3]**[6.2]	**[7]**[6.4]
[SW_Cactus] Biodata	**[7]**[2]	**[6]**[1]	**[5]**[6]	**[7]**[9]
[SW_Tarant]tarantela nomina	**[9]**[4]	**[9]**[6.3]	**[5]**[6]	**[9]**[4]
[SW_Aport] Aportes	**[9]**[6.2]	**[9]**[8]	**[7]**[3.1]	**[9]**[8]

[SW_os]sistemas operativos	**[7]**[1]	**[7]**[1]	**[7]**[1]	**[7]**[1]
[SW_av]antivirus	**[3]**[1]			**[7]**[5]
[SW_Edpro] Editores para el diseño y programación	**[3]**[1]			**[7]**[5]
[SW_dbms] sistemas de gestión de bases de datos	**[10]**[1]	**[10]**[3]	**[9]**[5]	**[9]**[8]
[SW_lengpro] lenguaje o plataforma de programación	**[3]**[1]			**[7]**[5]
[SW_browser] navegador web	**[7]**[1]			**[7]**[5]
[Sw_email] servicios de correo	**[3]**[1]			**[7]**[5]
[Sw_office] Ofimática	**[7]**[1]			**[7]**[1]
[ui] Usuarios Internos	**[7]**[1]			
[P-Adm] Administradores de Sistemas	**[9]**[1]			
[P-Com] Administradores de Comunicaciones	**[9]**[1]			
[P-DBa] Administradores de Bases de Datos	**[9]**[1]			
[P-Desrr] Desarrolladores	**[3]**[1]			
[P_C_Acd] Coordinador académico	**[9]**[1]			
[P_SDir] Subdirector de Centro	**[9]**[1]			
[P_C_Pro] Coordinadora de formación profesional	**[9]**[1]			
[P_C_admin] Coordinador Administrativo	**[9]**[1]			
[P_C_TH] Talento Humano	**[7]**[1]			
[ue] Usuarios externos	**[7]**[1]			

[HW_S] Servidores	**[9]**[1]			
[HW_PC] Informática personal	**[2]**[3]			
[HW_PRINT] Medios de impresión	**[2]**[3]			
[HW_switch] Conmutadores	**[5]**[1]			
[HW_router] Encaminadores	**[5]**[1]			
[HW_Cons] Consola de Descarga y video conferencia	**[3]**[1]			
[HW_Acces] Access point	**[3]**[1]			
[HW_Escan] Scanner	**[2]**[3]			
[HW _furniture] Mobiliario: Armarios, etc.	**[0]**[2]			
[COM_PSTN] Red Telefónica	**[7]**[1]			
[COM_radio] Red Inalámbrica	**[7]**[1]			
[COM_micro] Microondas	**[5]**[1]			
[COM_Red] Red	**[9]**[1]			
[COM_Internet] Internet	**[9]**[1]			
[CD] Cd-Rom	**[7]**[8]			
[usb]Dispositivos USB	**[7]**[8]			
[tape] Cinta Magnética	**[7]**[8]			
[Disk] Discos Duros	**[7]**[8]			
[printed] Material Impreso	**[7]**[8]			
[AUX _ups] Sistemas de Alimentación Ininterrumpida	**[5]**[1]			
[AUX _gen] Generadores Eléctricos	**[7]**[1]			

[AUX _ac] Equipos de Climatización	**[5]**[1]			
[AUX _cabling] Cableado	**[7]**[1]			
[AUX _armario]armario archivador	**[1]**[5]			

CRITERIOS DE VALORACIÓN

La valoración de los activos se realizara en forma cualitativa, respondiendo a criterios subjetivos. Se ha elegido una escala detallada de diez valores, tomando el valor 0 como determinante de lo que sería un valor despreciable a efectos de riesgo y 10 como valor muy alto.

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

VALOR	CRITERIO
10	**[1]**Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística. **[2]**Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información **[3]**Seguridad: probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios **[4]**Seguridad de las personas: probablemente suponga gran pérdida de vidas humanas **[5]**Orden público: alteración seria del orden constitucional. **[6]**Probablemente cause un impacto excepcionalmente grave en las relaciones internacionales. **[7]**Datos clasificados como secretos.
9	**[1]**Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización. **[2]**Administración y gestión: probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre. **[3]**Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones ... **[3.1]**A las relaciones con otras organizaciones. **[3.2]**A las relaciones con el público en general. **[3.3]**a las relaciones con otros países. **[4]**Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística. **[5]**Probablemente cause serios daños a misiones muy importantes de inteligencia o información. **[6]**Intereses comerciales o económicos: **[6.1]** De muy elevado valor comercial. **[6.2]**Causa de pérdidas económicas excepcionalmente elevadas. **[6.3]**Causa de muy significativas ganancias o ventajas para

	Individuos u organizaciones. **[7]**Obligaciones legales: probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación. **[8]**Seguridad: probablemente sea causa de un serio incidente de seguridad (Beneficios a algún(os) individuo de la empresa o robo). **[9]**Seguridad de las personas: probablemente suponga la muerte de uno o más individuos. **[10]**Orden público: alteración seria del orden público. **[11]**Probablemente cause un serio impacto en las relaciones internacionales. **[12]**Datos clasificados como reservados.
8	**[1]**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 más individuos). **[2]**Impida la investigación de delitos graves o facilite su comisión. **[3]**Datos clasificados como confidenciales.
7	**[1]**Probablemente cause una interrupción seria de las actividades propias de la Organización. **[2]**Administración y gestión: probablemente impediría la operación efectiva de la organización. **[3]**Probablemente causaría una publicidad negativa generalizada. **[3.1]**Por afectar gravemente a las relaciones con otras organizaciones **[3.2]**Por afectar gravemente a las relaciones con el público en general **[3.3]**Por afectar gravemente a las relaciones con otros países. **[4]**Probablemente cause perjudique la eficacia o seguridad de la misión operativa o logística. **[5]**Probablemente cause serios daños a misiones importantes de inteligencia o información. **[6]**Intereses comerciales o económicos: **[6.1]**De alto interés para la competencia.

	[6.2]De elevado valor comercial. **[6.3]**Causa de graves pérdidas económicas. **[6.4]**Proporciona ganancias o ventajas desmedidas a Individuos u organizaciones. **[6.5]**Constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros. **[7]**Obligaciones legales: probablemente cause un incumplimiento grave de una ley o regulación. **[8]**Seguridad: probablemente sea causa de un grave incidente de seguridad (ejecución de tareas no deseadas, robo de contraseñas). **[9]**Seguridad de las personas: probablemente cause daños de cierta consideración a varios individuos. **[10]**Probablemente cause un impacto significativo en las relaciones internacionales. **[11]** Datos clasificados como confidenciales.
6	**[1]**Información personal: probablemente afecte gravemente a un grupo de individuos. **[2]**Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal. **[3]**Seguridad de las personas: probablemente cause daños de cierta consideración, restringidos a un individuo. **[4]**Orden público: probablemente cause manifestaciones, o presiones significativas. **[5]**Datos clasificados como de difusión limitada.
5	**[1]**Probablemente cause la interrupción de actividades propias de la Organización. **[2]**Administración y gestión: probablemente impediría la operación efectiva de más de una parte de la organización. **[3]**Probablemente sea causa una cierta publicidad negativa. **[3.1]**Por afectar negativamente a las relaciones con otras organizaciones.

	[3.2] por afectar negativamente a las relaciones con el público. **[4]**Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local. **[5]**Probablemente dañe a misiones importantes de inteligencia o información. **[6]**Información personal: probablemente afecte gravemente a un individuo. **[7]**Información personal: probablemente quebrante seriamente leyes o regulaciones. **[8]**Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación. **[9]**Probablemente tenga impacto en las relaciones internacionales. **[10]**Datos clasificados como de difusión limitada.
4	**[1]**Información personal: probablemente afecte a un grupo de individuos. **[2]**Información personal: probablemente quebrante leyes o regulaciones. **[3]**Seguridad de las personas: probablemente cause daños menores a varios individuos. **[4]**Dificulte la investigación o facilite la comisión de delitos. **[5]**Datos clasificados como de difusión limitada.
3	**[1]**Probablemente cause la interrupción de actividades propias de la Organización. **[2]**Administración y gestión: probablemente impediría la operación efectiva de una parte de la organización. **[3]**Probablemente afecte negativamente a las relaciones internas de la Organización. **[4]**Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local). **[5]**Probablemente cause algún daño menor a misiones importantes de inteligencia o información.

	[6]Intereses comerciales o económicos: **[6.1]**De cierto interés para la competencia. **[6.2]**De cierto valor comercial. **[6.3]**Causa de pérdidas financieras o merma de ingresos. **[6.4]**Facilita ventajas desproporcionadas a individuos u Organizaciones. **[6.5]**Constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros. **[7]**Información personal: probablemente afecte a un individuo. **[8]**Información personal: probablemente suponga el incumplimiento de una ley o regulación. **[9]**Obligaciones legales: probablemente sea causa de incumplimiento leve o técnico de una ley o regulación. **[10]**Seguridad: probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente. **[11]**Seguridad de las personas: probablemente cause daños menores a un individuo. **[12]**Orden público: causa de protestas puntuales. **[13]**Probablemente cause un impacto leve en las relaciones internacionales. **[14]**Datos clasificados como de difusión limitada.
2	**[1]**Probablemente cause una pérdida menor de la confianza dentro de la Organización. **[2]**Intereses comerciales o económicos: **[2.1]**De bajo interés para la competencia. **[2.2]**De bajo valor comercial. **[3]**Información personal: pudiera causar retraso a un individuo u organización. **[4]**Información personal: pudiera quebrantar de forma leve leyes o

	regulaciones. **[5]**Seguridad de las personas: pudiera causar daño menor a varios individuos. **[6]**Datos clasificados como sin clasificar.
1	**[1]**Pudiera causar la interrupción de actividades propias de la Organización. **[2]**Administración y gestión: pudiera impedir la operación efectiva de una parte de la organización. **[3]**Pudiera causar una pérdida menor de la confianza dentro de la Organización. **[4]**Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local). **[5]**Pudiera causar algún daño menor a misiones importantes de inteligencia o información. **[6]**Intereses comerciales o económicos: **[6.1]**De pequeño interés para la competencia. **[6.2]**De pequeño valor comercial. **[7]**Información personal: pudiera causar molestias a un individuo. **[8]**Obligaciones legales: pudiera causar el incumplimiento leve o técnico de una ley o regulación. **[9]**Seguridad: pudiera causar una merma en la seguridad o dificultar la investigación de un incidente. **[10]**Seguridad de las personas: pudiera causar daños menores a un individuo. **[11]**Orden público: pudiera causar protestas puntuales. **[12]**Pudiera tener un impacto leve en las relaciones internacionales. **[13]**Datos clasificados como sin clasificar.
	[1]No afectaría a la seguridad de las personas. **[2]**Sería causa de inconveniencias mínimas a las partes afectadas.

0	**[3]**Supondría pérdidas económicas mínimas. **[4]**No supondría daño a la reputación o buena imagen de las personas u organizaciones.

AMENAZAS DE ACTIVOS

A continuación conoceremos las amenazas de las que pueden ser víctimas los activos del Tic Solution. Se entiende por amenaza a la posible ocurrencia todo hecho que puede causar daños a los diferentes tipos de activos de la organización.

[N] Desastres Naturales.

[N.1] Fuego	
Tipos de activos afectados •[HW] equipos informáticos (hardware). •[COM] redes de comunicaciones. •[SI] soportes de información. •[AUX] equipamiento auxiliar. •[L] instalaciones.	**Dimensiones**: 1.[D] disponibilidad
Descripción: Incendios: posibilidad de que el fuego acabe con recursos del sistema del Tic Solution Tic Solution.	

[N.2] Daños por agua	
Tipos de activos afectados •[HW] equipos informáticos (hardware) •[COM] redes de comunicaciones •[SI] soportes de información •[AUX] equipamiento auxiliar •[L] instalaciones	**Dimensiones**: 1.[D] disponibilidad

Descripción:
Posibilidad de que el agua acabe con recursos del sistema, dado que puedan presentarse Inundaciones por causa de lluvia en las instalaciones del Tic Solution.

[N.*] Desastres Naturales	
Tipos de activos afectados •[HW] equipos informáticos (hardware) •[COM] redes de comunicaciones •[SI] soportes de información •[AUX] equipamiento auxiliar •[L] instalaciones	**Dimensiones**: 1.[D] disponibilidad
Descripción: Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, entre otros desastres naturales que causen avería y daños a las instalaciones de Tic Solution.	

[I] De origen industrial.

[I.1] Fuego	
Tipos de activos afectados • [HW] equipos informáticos (hardware). • [COM] redes de comunicaciones. • [SI] soportes de información. • [AUX] equipamiento auxiliar. • [L] instalaciones.	**Dimensiones**: 1.[D] disponibilidad
Descripción: Incendio: posibilidad de que el fuego acabe con los recursos del sistema, dado que en las instalaciones del Tic Solution se cuenta con laboratorios se utiliza material inflamable.	

[I.2] Daños por agua

Tipos de activos afectados	Dimensiones:
•[HW] equipos informáticos (hardware) •[COM] redes de comunicaciones •[SI] soportes de información •[AUX] equipamiento auxiliar •[L] instalaciones	1.[D] disponibilidad
Descripción: Inundaciones: posibilidad de que el agua acabe con recursos del sistema.	

[I.*] Desastres industriales	
Tipos de activos afectados	**Dimensiones:**
•[HW] equipos informáticos (hardware) •[COM] redes de comunicaciones •[SI] soportes de información •[AUX] equipamiento auxiliar •[L] instalaciones	1.[D] disponibilidad
Descripción: Otros desastres debidos a la actividad humana: explosiones, derrumbes,... contaminación química,... sobrecarga eléctrica, fluctuaciones eléctricas,... accidentes de tráfico,...	

[I.5] Avería de origen físico o lógico	
Tipos de activos afectados	**Dimensiones:**
•[SW] aplicaciones (software) •[HW] equipos informáticos (hardware) •[COM] redes de comunicaciones •[SI] soportes de información •[AUX] equipamiento auxiliar	1.[D] disponibilidad
Descripción: Fallos en los equipos y fallos en los programas. Puede ser debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema.	

[I.6] Corte del subministro eléctrico	
Tipos de activos afectados •[HW] equipos informáticos (hardware) •[COM] redes de comunicaciones •[SI] soportes de información (electrónicos) •[AUX] equipamiento auxiliar	**Dimensiones:** 1.[D] disponibilidad
Descripción: Cese de la alimentación de potencia. En el caso de que se explote algún transformador o generador eléctrico, como también se dispare o se averié alguna cuña eléctrica.	

[I.7] Condiciones inadecuadas de temperatura y/o humedad	
Tipos de activos afectados •[HW] equipos informáticos (hardware) •[COM] redes de comunicaciones •[SI] soportes de información •[AUX] equipamiento auxiliar	**Dimensiones:** 1.[D] disponibilidad
Descripción: Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad,...	

[I.8] Fallo de servicios de comunicaciones

Tipos de activos afectados	Dimensiones:
•[COM] redes de comunicaciones	1.[D] disponibilidad
Descripción: Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente. Fallos del proveedor de servicio de Internet, daños en los dispositivos d comunicación de la red.	

[I.10] Degradación de los soportes de almacenamiento de la información	
Tipos de activos afectados	**Dimensiones:**
•[SI] soportes de información	1.[D] disponibilidad
Descripción: Como consecuencia del paso del tiempo estos se pueden averiar.	

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios	
Tipos de activos afectados	**Dimensiones:**
• [S] servicios • [D] datos / información • [SW] aplicaciones (software)	1. [I] integridad 2. [D] disponibilidad
Descripción: Equivocaciones de las personas cuando usan los servicios, datos, aplicaciones. Ingresando, modificando o eliminando algunos de estos activos por algún desliz.	

[E.2] Errores del administrador

Tipos de activos afectados	**Dimensiones:**
• [S] servicios • [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A] autenticidad
Descripción: Equivocaciones de personas con responsabilidades de instalación y operación en la parte administrativa, como en el desarrollo de las aplicaciones, y en el mantenimiento de los equipos.	

[E.4] Errores de configuración	
Tipos de activos afectados	Dimensiones:
• [S] servicios • [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A] autenticidad
Descripción: Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento.	

[E.8] Difusión de software dañino

Tipos de activos afectados	Dimensiones:
• [SW] aplicaciones (software)	1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A] autenticidad
Descripción: Propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, crackers y hackers.	

[E.9] Errores de [re-]encaminamiento	
Tipos de activos afectados	**Dimensiones:**
• [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	1. [C] confidencialidad 2. [I] integridad 3. [A] autenticidad
Descripción: Cuando se envía información por medio de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.	

[E.14] Escapes de información	
Tipos de activos afectados	**Dimensiones:**
• [D] datos / información • [SW] aplicaciones (software) • [COM] redes de comunicaciones	1. [C] confidencialidad
Descripción: La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que esta en sí misma se vea alterada.	

[E.15] Alteración de la información	
Tipos de activos afectados • [D] datos / información	**Dimensiones:** 1. [I] Integridad
Descripción: Modificación accidental de la información por parte de las personas o usuarios que quieren acceder a ella de manera intencional.	

[E.16] Introducción de información incorrecta	
Tipos de activos afectados • [D] datos / información	**Dimensiones:** 1. [I] Integridad
Descripción: Inserción accidental de información incorrecta.	

[E.17] Degradación de la información	
Tipos de activos afectados • [D] datos / información	**Dimensiones** 1. [I] Integridad
Descripción: Degradación accidental de la información.	

[E.18] Destrucción de información	
Tipos de activos afectados • [D] datos / información	**Dimensiones:** 1. [D] disponibilidad
Descripción: Pérdida accidental de información por parte del personal.	

[E.19] Divulgación de información	
Tipos de activos afectados • [D] datos / información	**Dimensiones:** 1. [C] confidencialidad
Descripción: Revelación por indiscreción. Imprudencia al revelar información del centro. Incontinencia verbal, medios electrónicos, soporte papel, etc.	

[E.20] Vulnerabilidades de los programas (software)	
Tipos de activos afectados • [SW] aplicaciones (software)	**Dimensiones:** 1. [I] integridad 2. [D] disponibilidad 3. [C] confidencialidad
Descripción: Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	

[E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos afectados • [SW] aplicaciones (software)	**Dimensiones** 1. [I] integridad 2. [D] disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	

Tipos de activos afectados	Dimensiones:
• [HW] equipos informáticos (hardware)	1. [D] disponibilidad
Descripción: Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso. Causando deterioros en ellos y mal funcionamiento.	

[E.24] Caída del sistema por agotamiento de recursos	
Tipos de activos afectados	**Dimensiones:**
• [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	1. [D] disponibilidad
Descripción: La carencia de equipos sofisticados y suficientes que resistan la comunicación del Tic Solution.	

[E.28] Indisponibilidad del personal	
Tipos de activos afectados	**Dimensiones:**
• [P_ui] personal interno	1. [D] disponibilidad
Descripción: Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, paros, huelgas que se presentan ocasionalmente en el TIC SOLUTION	

[A] Ataques intencionados

[A.4] Manipulación de la configuración	
Tipos de activos afectados • [S] servicios • [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [A] autenticidad 4. [D] disponibilidad
Descripción: Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	

[A.5] Suplantación de la identidad del usuario	
Tipos de activos afectados • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad 3. [A] autenticidad
Descripción: Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	

[A.6] Abuso de privilegios de acceso	
Tipos de activos afectados • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (Hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad 2. [C] confidencialidad
Descripción: Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia y autorizadas, trae problemas y consecuencias.	

[A.7] Uso no previsto	
Tipos de activos afectados • [S] servicios • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.	

[A.8] Difusión de software dañino	
Tipos de activos afectados • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad 4. [A] autenticidad
Descripción: Propagación intencionada de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, crackers y hacker.	

[A.10] Alteración de secuencia	
Tipos de activos afectados • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [I] integridad
Descripción: Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.	

[A.11] Acceso no autorizado	
Tipos de activos afectados • [S] servicios • [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A] autenticidad

Descripción:
El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

[A.12] Análisis de tráfico	
Tipos de activos afectados • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios. A veces se denomina “monitorización de tráfico”.	

[A.14] Interceptación de información (escucha)	
Tipos de activos afectados • [D] datos / información • [SW] aplicaciones (software) • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	

[A.15] Modificación de la información	
Tipos de activos afectados • [D] datos / información	**Dimensiones:** 1. [I] Integridad
Descripción: Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	

[A.16] Introducción de falsa información	
Tipos de activos afectados • [D] datos / información	**Dimensiones:** 1. [I] Integridad
Descripción: Inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio.	

[A.17] Corrupción de la información	
Tipos de activos afectados • [D] datos / información	**Dimensiones:** 1. [I] Integridad
Descripción: Degradación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	

[A.18] Destrucción la información	
Tipos de activos afectados • [D] datos / información	**Dimensiones:** 1. [D] disponibilidad
Descripción: Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	

[A.19] Divulgación de información	
Tipos de activos afectados • [D] datos / información	**Dimensiones:** 1. [C] confidencialidad
Descripción: Revelación de información confidencial o reservada que se maneja en el TIC	

SOLUTION

[A.22] Manipulación de programas	
Tipos de activos afectados • [SW] aplicaciones (software)	**Dimensiones:** 1. [C] confidencialidad 2. [I] integridad 3. [A] autenticidad
Descripción: Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	

[A.24] Denegación de servicio	
Tipos de activos afectados • [S] servicios • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones	**Dimensiones:** 1. [D] disponibilidad
Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	
[A.25] Robo	
Tipos de activos afectados • [HW] equipos informáticos (hardware) • [COM] redes de comunicaciones • [SI] soportes de información • [AUX] equipamiento auxiliar	**Dimensiones:** 1. [D] disponibilidad 2. [C] confidencialidad
Descripción: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o	

personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

[A.28] Indisponibilidad del personal	
Tipos de activos afectados • [P_ui] personal interno	**Dimensiones:** 1. [D] disponibilidad
Descripción: Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos,...	

IMPACTO Y RIESGO

tabla de frecuencia	Escala
1	bajo
2	medio
3	alto

Tipos de riesgo	Rango
Trivial	[0- 4]
Tolerable	[5- 8]
Moderado	[9 – 13]
Importante	[14 – 17]
Intolerable	[18 – 21]

Aplicaciones

ACTIVOS/AMENAZAS	Valor	Dimen				
[SW_Fin2000] Finanzas2000	7	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	1	Trivial
[E.4] Errores de configuración		60%	1	4	4	Trivial

[E.8] Difusión de software dañino		70%	3	5	15	Importante
[A.4] Manipulación de la configuración		65%	1	5	5	Tolerable
[A.8] Difusión de software dañino		70%	1	5	5	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	4	4	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	5	5	Tolerable
	7	**[I]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.20] Vulnerabilidades de los programas (software)		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		70%	1	5	5	Tolerable
	3	**[c]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		50%	1	2	2	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	2	2	Trivial
[A.4] Manipulación de la configuración		50%	1	2	2	Trivial
[A.5] Suplantación de la identidad del usuario		90%	1	3	3	Trivial
	9	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	6	6	Tolerable
[E.4] Errores de configuración		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		70%	1	6	6	Tolerable
	9	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	6	6	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	5	5	Tolerable
[SW_Spem] Servicio público de empleo	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.4] Errores de configuración		60%	1	5	5	Tolerable
[E.8] Difusión de software dañino		70%	3	6	18	Importante
[A.4] Manipulación de la configuración		65%	1	6	6	Tolerable
[A.8] Difusión de software dañino		70%	1	6	6	Tolerable
[E.20] Vulnerabilidades de los programas(software)		70%	1	6	6	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	5	5	Tolerable

[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
	9	**[I]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		70%	1	6	6	Tolerable
	9	**[c]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		50%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		50%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		90%	1	8	8	Tolerable
	6	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		70%	1	4	4	Tolerable
[A.4] Manipulación de la configuración		70%	1	4	4	Tolerable
[A.5] Suplantación de la identidad del usuario		70%	1	4	4	Trivial
	6	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	4	4	Trivial
[A.5] Suplantación de la identidad del usuario		60%	1	4	4	Trivial
[SW_web_regi] Pagina web de la regional Bolívar	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.4] Errores de configuración		60%	1	5	5	Tolerable
[E.8] Difusión de software dañino		70%	3	6	18	Importante
[A.4] Manipulación de la configuración		65%	1	6	6	Tolerable
[A.8] Difusión de software dañino		70%	1	6	6	Tolerable
[E.20] Vulnerabilidades de los programas(software)		70%	1	6	6	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
	9	**[I]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable

[A.4] Manipulación de la configuración		70%	1	6	6	Tolerable
	6	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		70%	1	4	4	Tolerable
[A.4] Manipulación de la configuración		70%	1	4	4	Tolerable
[A.5] Suplantación de la identidad del usuario		70%	1	4	4	Trivial
	6	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	4	4	Trivial
[A.5] Suplantación de la identidad del usuario		60%	1	4	4	Trivial
[SW_SAGC] sistema académico de gestión de centro	**10**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.4] Errores de configuración		60%	1	6	6	Tolerable
[E.8] Difusión de software dañino		70%	3	7	21	Intolerable
[A.4] Manipulación de la configuración		65%	1	7	7	Tolerable
[A.8] Difusión de software dañino		70%	1	7	7	Tolerable
[E.20] Vulnerabilidades de los programas(software)		70%	1	7	7	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas (software)		70%	1	7	7	Tolerable
	9	**[I]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		70%	1	6	6	Tolerable
	9	**[c]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		50%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		50%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		90%	1	8	8	Tolerable
	9	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		70%	1	6	6	Tolerable

[A.5] Suplantación de la identidad del usuario		70%	1	6	6	Tolerable
	9	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	6	6	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	5	5	Tolerable
[SW_SGVA] sistema de gestión virtual de aprendices	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.4] Errores de configuración		60%	1	5	5	Tolerable
[E.8] Difusión de software dañino		70%	3	6	18	Importante
[A.4] Manipulación de la configuración		65%	1	6	6	Tolerable
[A.8] Difusión de software dañino		70%	1	6	6	Tolerable
[E.20] Vulnerabilidades de los programas(software)		70%	1	6	6	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
	5	**[I]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.20] Vulnerabilidades de los programas (software)		70%	1	4	4	Trivial
[A.4] Manipulación de la configuración		70%	1	4	4	Trivial
	4	**[c]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		50%	1	2	2	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	3	3	Trivial
[A.4] Manipulación de la configuración		50%	1	2	2	Trivial
[A.5] Suplantación de la identidad del usuario		90%	1	4	4	Trivial
	4	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		70%	1	3	3	Tolerable
[A.4] Manipulación de la configuración		70%	1	3	3	Tolerable
[A.5] Suplantación de la identidad del usuario		70%	1	3	3	Trivial
	4	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**

[A.11] Acceso no autorizado		70%	1	3	3	Trivial
[A.5] Suplantación de la identidad del usuario		60%	1	2	2	Trivial
[SW_Adm2000] Administración 2000	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	1	Trivial
[E.4] Errores de configuración		60%	1	4	4	Trivial
[E.8] Difusión de software dañino		70%	3	5	15	Importante
[A.4] Manipulación de la configuración		65%	1	5	5	Tolerable
[A.8] Difusión de software dañino		70%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas(software)		70%	1	5	5	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	4	4	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	5	5	Tolerable
	7	**[I]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.20] Vulnerabilidades de los programas (software)		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		70%	1	5	5	Tolerable
	3	**[c]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		50%	1	2	2	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	2	2	Trivial
[A.4] Manipulación de la configuración		50%	1	2	2	Trivial
[A.5] Suplantación de la identidad del usuario		90%	1	3	3	Trivial
	7	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		70%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		70%	1	5	5	Tolerable
	7	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	4	4	Trivial

[SW_Cactus] Biodata	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	1	Trivial
[E.4] Errores de configuración		60%	1	4	4	Trivial
[E.8] Difusión de software dañino		70%	3	5	15	Importante
[A.4] Manipulación de la configuración		65%	1	5	5	Tolerable
[A.8] Difusión de software dañino		70%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas(software)		70%	1	5	5	
[E.21] Errores de mantenimiento / actualización		50%	1	4	4	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	5	5	Tolerable
	6	**[I]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.20] Vulnerabilidades de los programas (software)		70%	1	4	4	Trivial
[A.4] Manipulación de la configuración		70%	1	4	4	Trivial
	5	**[c]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		50%	1	3	3	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	4	4	Trivial
[A.4] Manipulación de la configuración		50%	1	3	3	Trivial
[A.5] Suplantación de la identidad del usuario		90%	1	5	5	Tolerable
	7	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	5	5	Tolerable
[E.4] Errores de configuración		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		70%	1	5	5	Tolerable
	7	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	4	4	Trivial
[SW_Tarant]tarantela nomina	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.4] Errores de configuración		60%	1	5	5	Tolerable

[E.8] Difusión de software dañino		70%	3	6	18	Importante
[A.4] Manipulación de la configuración		65%	1	6	6	Tolerable
[A.8] Difusión de software dañino		70%	1	6	6	Tolerable
[E.20] Vulnerabilidades de los programas(software)		70%	1	6	6	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
	9	**[I]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		70%	1	6	6	Tolerable
	5	**[c]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		50%	1	3	3	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	4	4	Trivial
[A.4] Manipulación de la configuración		50%	1	3	3	Trivial
[A.5] Suplantación de la identidad del usuario		90%	1	5	5	Tolerable
	9	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	6	6	Tolerable
[E.4] Errores de configuración		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		70%	1	6	6	Tolerable
	9	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	6	6	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	5	5	Tolerable
[SW_Aport] Aportes	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.4] Errores de configuración		60%	1	5	5	Tolerable
[E.8] Difusión de software dañino		70%	3	6	18	Importante
[A.4] Manipulación de la configuración		65%	1	6	6	Tolerable
[A.8] Difusión de software dañino		70%	1	6	6	Tolerable

[E.20] Vulnerabilidades de los programas(software)		70%	1	6	6	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
	9	**[I]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		70%	1	6	6	Tolerable
	7	**[c]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		50%	1	4	4	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		50%	1	4	4	Trivial
[A.5] Suplantación de la identidad del usuario		90%	1	6	6	Tolerable
	9	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	6	6	Tolerable
[E.4] Errores de configuración		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		70%	1	6	6	Tolerable
	9	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	6	6	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	5	5	Tolerable
ACTIVOS/AMENAZAS	**Valor**	**Dimen**				
[SW_os]sistemas operativos	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	1	Trivial
[E.4] Errores de configuración		60%	1	4	4	Trivial
[E.8] Difusión de software dañino		70%	3	5	15	Importante
[A.4] Manipulación de la configuración		65%	1	5	5	Tolerable
[A.8] Difusión de software dañino		70%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas(software)		70%	1	5	5	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	4	4	Trivial
[E.20] Vulnerabilidades de los programas		70%	1	5	5	Tolerable

(software)						
	7	**[I]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.20] Vulnerabilidades de los programas (software)		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		70%	1	5	5	Tolerable
	7	**[c]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		50%	1	4	4	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		50%	1	4	4	Tolerable
[A.5] Suplantación de la identidad del usuario		90%	1	6	6	Tolerable
	7	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	5	5	Tolerable
[E.4] Errores de configuración		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		70%	1	6	6	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	4	4	Trivial
[SW_av]antivirus	3	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	0	0	Trivial
[E.4] Errores de configuración		60%	1	2	2	Trivial
[E.8] Difusión de software dañino		70%	3	2	6	Tolerable
[A.4] Manipulación de la configuración		65%	1	2	2	Trivial
[A.8] Difusión de software dañino		70%	1	2	2	Trivial
[E.20] Vulnerabilidades de los programas(software)		70%	1	2	2	Trivial
[E.21] Errores de mantenimiento / actualización		50%	1	2	2	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	2	2	Trivial
	7	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	5	5	Tolerable
[E.4] Errores de configuración		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		70%	1	5	5	Tolerable

	7	[A_S]	Fre	Impac	Riesgo	Tipo riego
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	4	4	Trivial
[SW_Edpro] Editores para el diseño y programación	**3**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	0	0	Trivial
[E.4] Errores de configuración		60%	1	2	2	Trivial
[E.8] Difusión de software dañino		70%	3	2	6	Tolerable
[A.4] Manipulación de la configuración		65%	1	2	2	Trivial
[A.8] Difusión de software dañino		70%	1	2	2	Trivial
[E.20] Vulnerabilidades de los programas(software)		70%	1	2	2	Trivial
[E.21] Errores de mantenimiento / actualización		50%	1	2	2	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	2	2	Trivial
	7	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	5	5	Tolerable
[E.4] Errores de configuración		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		70%	1	5	5	Tolerable
	7	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	4	4	Trivial
[SW_dbms] sistemas de gestión de bases de datos	**10**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.4] Errores de configuración		60%	1	6	6	Tolerable
[E.8] Difusión de software dañino		70%	3	7	21	Intolerable
[A.4] Manipulación de la configuración		65%	1	7	7	Tolerable
[A.8] Difusión de software dañino		70%	1	7	7	Tolerable
[E.20] Vulnerabilidades de los programas(software)		70%	1	7	7	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas		70%	1	7	7	Tolerable

(software)						
	10	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.20] Vulnerabilidades de los programas (software)		70%	1	7	7	Tolerable
[A.4] Manipulación de la configuración		70%	1	7	7	Tolerable
	9	**[c]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.4] Errores de configuración		50%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas (software)		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		50%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		90%	1	8	8	Tolerable
	9	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	6	6	Tolerable
[E.4] Errores de configuración		70%	1	6	6	Tolerable
[A.4] Manipulación de la configuración		70%	1	6	6	Tolerable
	9	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	6	6	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	5	5	Tolerable
[SW_browser] navegador web	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.4] Errores de configuración		60%	1	4	4	Trivial
[E.8] Difusión de software dañino		70%	3	5	15	Importante
[A.4] Manipulación de la configuración		65%	1	5	5	Tolerable
[A.8] Difusión de software dañino		70%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas(software)		70%	1	5	5	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	4	4	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	5	5	Tolerable
	7	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	5	5	Tolerable
[E.4] Errores de configuración		70%	1	5	5	Tolerable

[A.4] Manipulación de la configuración		70%	1	5	5	Tolerable
	7	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	4	4	Trivial
[Sw_email] servicios de correo	3	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	0	0	Trivial
[E.4] Errores de configuración		60%	1	2	2	Trivial
[E.8] Difusión de software dañino		70%	3	2	6	Tolerable
[A.4] Manipulación de la configuración		65%	1	2	2	Trivial
[A.8] Difusión de software dañino		70%	1	2	2	Trivial
[E.20] Vulnerabilidades de los programas(software)		70%	1	2	6	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	2	2	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	2	2	Trivial
	7	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	5	5	Tolerable
[E.4] Errores de configuración		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		70%	1	5	5	Tolerable
	7	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	4	4	Trivial
[Sw_office] Ofimática	7	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.4] Errores de configuración		60%	1	4	4	Trivial
[E.8] Difusión de software dañino		70%	3	5	15	Importante
[A.4] Manipulación de la configuración		65%	1	5	5	Tolerable
[A.8] Difusión de software dañino		70%	1	5	5	Tolerable
[E.20] Vulnerabilidades de los programas(software)		70%	1	5	5	Tolerable
[E.21] Errores de mantenimiento / actualización		50%	1	4	4	Trivial
[E.20] Vulnerabilidades de los programas		70%	1	5	5	Tolerable

(software)						
	7	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	5	5	Tolerable
[E.4] Errores de configuración		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		70%	1	5	5	Tolerable
	7	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	4	4	Trivial
[SW_lengpro] lenguaje o plataforma de programación	**3**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		10%	2	0	0	Trivial
[E.4] Errores de configuración		60%	1	2	2	Trivial
[E.8] Difusión de software dañino		70%	3	2	6	Tolerable
[A.4] Manipulación de la configuración		65%	1	2	2	Trivial
[A.8] Difusión de software dañino		70%	1	2	2	Trivial
[E.20] Vulnerabilidades de los programas(software)		70%	1	2	2	Trivial
[E.21] Errores de mantenimiento / actualización		50%	1	2	2	Trivial
[E.20] Vulnerabilidades de los programas (software)		70%	1	2	2	Trivial
	7	**[A_D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.5] Suplantación de la identidad del usuario		70%	1	5	5	Tolerable
[E.4] Errores de configuración		70%	1	5	5	Tolerable
[A.4] Manipulación de la configuración		70%	1	5	5	Tolerable
	7	**[A_S]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.5] Suplantación de la identidad del usuario		60%	1	4	4	Trivial

Servicios

ACTIVOS/AMENAZAS	Valor	Dimen				
[S_Capacit] Servicio de capacitación y formación	**10**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riesgo**
[E.1] Errores de los usuarios		70%	2	7	14	Importante
[A.24] Denegación de servicio		100%	1	10	10	Moderado
[E.24] Caída del sistema por agotamiento de recursos		70%	1	7	7	Tolerable
[S_Aten] Atención a la demanda educativa	**10**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		70%	2	7	14	Importante
[A.24] Denegación de servicio		100%	1	10	10	Moderado
[S_Recorp] Relacionamiento Corporativo	**3**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		70%	2	6	12	Moderado
[A.24] Denegación de servicio		80%	1	2	2	Trivial
[A.5] Suplantación de la identidad del usuario		60%	1	3	3	Trivial
[S_InforWeb] Información en el portal Web	**1**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[A.24] Denegación de servicio		100%	1	1	1	Trivial
[E.24] Caída del sistema por agotamiento de recursos		40%	1	0	0	Trivial
[S_C_cont] compras y contratación	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		60%	2	4	8	Tolerable
[A.24] Denegación de servicio		100%	1	7	7	Tolerable
	9	**[A]**	**Fre**	**Impac**	**Riesgo**	
[A.5] Suplantación de la identidad del usuario		70%	1	6	6	Tolerable

[S_C_Acad] Servicio de coordinación	**10**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		50%	2	5	10	Moderado
[A.24] Denegación de servicio		90%	1	9	9	Moderado
[S_C_ForP] Coordinación De Formación Profesional	**4**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[A.24] Denegación de servicio		100%	1	4	4	Trivial
[E.1] Errores de los usuarios		50%	2	2	4	Trivial
	2	**[A]**	**Fre**	**Impac**	**Riesgo**	
[S_RegC] Registro y Certificación de alumnos	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		50%	2	5	10	Moderado
[A.24] Denegación de servicio		80%	1	7	7	Tolerable
[S_Adm_R_BD]Administración de red y base de datos	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		20%	2	2	4	
[E.2] Errores del administrador		70%	1	6	6	Tolerable
[E.4] Errores de configuración		70%	1	6	6	Tolerable
	9	**[A]**	**Fre**	**Impac**	**Riesgo**	
[E.2] Errores del administrador		70%	1	6	6	Tolerable
[E.4] Errores de configuración		70%	1	6	6	Tolerable
[S_soport]Soporte técnico	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.2] Errores del administrador		80%	1	6	6	Tolerable
[E.4] Errores de configuración		70%	1	5	5	Tolerable
	1	**[A]**	**Fre**	**Impac**	**Riesgo**	
[E.2] Errores del administrador		70%	1	1	1	Trivial
[E.4] Errores de configuración		70%	1	1	1	Trivial

[S_Di_web]Diseño y administración de pagina web	**1**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.2] Errores del administrador		30%	1	0	0	Trivial
[E.4] Errores de configuración		60%	1	1	1	Trivial
[A.24] Denegación de servicio		100%	1	1	1	Trivial
ACTIVOS/AMENAZAS	**Valor**	**Dimen**				
[S_Di_web]Diseño y administración de página web	**1**	**[A]**	**Fre**	**Impac**	**Riesgo**	**Tipo riesgo**
[E.2] Errores del administrador		70%	1	1	1	Trivial
[E.4] Errores de configuración		70%	1	1	1	Trivial
[S_DHCP] Asignación de direcciones dinámicas	**5**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.2] Errores del administrador		70%	1	4	4	Trivial
[E.4] Errores de configuración		70%	1	4	4	Trivial
[E.24] Caída del sistema por agotamiento de recursos		70%	1	4	4	Trivial
[A.4] Manipulación de la configuración		80%	1	4	4	Trivial
[A.24] Denegación de servicio		100%	1	5	5	Tolerable
	3	**[A]**	**Fre**	**Impac**	**Riesgo**	
[E.2] Errores del administrador		50%	1	2	2	Trivial
[E.4] Errores de configuración		60%	1	2	2	Trivial
[A.4] Manipulación de la configuración		70%	1	2	2	Trivial
[A.5] Suplantación de la identidad del usuario		60%	1	2	2	Trivial
[A.11] Acceso no autorizado		80%	1	2	2	Trivial
[S_ Ftp] Transferencia de archivos	**5**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.2] Errores del administrador		80%	1	4	4	Trivial
[E.4] Errores de configuración		80%	1	4	4	Trivial

[E.24] Caída del sistema por agotamiento de recursos		70%	1	4	4	Trivial
[A.4] Manipulación de la configuración		80%	1	4	4	Trivial
[A.24] Denegación de servicio		100%	1	5	5	Tolerable
	4	**[A]**	**Fre**	**Impac**	**Riesgo**	
[E.2] Errores del administrador		70%	1	3	3	Trivial
[E.4] Errores de configuración		70%	1	3	3	Trivial
[A.4] Manipulación de la configuración		60%	1	2	2	Trivial
[A.5] Suplantación de la identidad del usuario		80%	1	3	3	Trivial
[A.11] Acceso no autorizado		70%	1	3	3	Trivial
[S_ LiqNom] Liquidación de nomina	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		20%	2	1	2	Trivial
	3	**[A]**	**Fre**	**Impac**	**Riesgo**	
[A.11] Acceso no autorizado		70%	1	2	2	Trivial
[S_Mant_p_e] Servicio de mto de planta y equipos	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		20%	2	1	2	Trivial
[E.2] Errores del administrador		70%	1	5	5	Tolerable
	1	**[A]**	**Fre**	**Impac**	**Riesgo**	
[E.2] Errores del administrador		70%	1	1	1	Trivial
[S_Inst] Instructores contratistas	**5**	**[A]**	**Fre**	**Impac**	**Riesgo**	
[A.5] Suplantación de la identidad del usuario		80%	1	4	4	Trivial
ACTIVOS/AMENAZAS	**Valor**	**Dimen**				
[S_Internet] Internet	**10**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riesgo**
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.2] Errores del administrador		80%	1	8	8	Tolerable
[E.4] Errores de configuración		90%	1	9	9	Moderado

[E.24] Caída del sistema por agotamiento de recursos		90%	2	9	18	Intolerable
[A.4] Manipulación de la configuración		90%	1	9	9	Moderado
[A.7] Uso no previsto		20%	3	2	6	Tolerable
[A.24] Denegación de servicio		90%	1	9	9	Moderado

Datos

ACTIVOS	Valor	Dimen				
[D_R_MIns] Reportes mensuales de instructores	**9**	**[I]**	**Fre**	**Impac**	**Riesgo**	**Tipo Riesgo**
[A.15] Modificación de información		80%	1	7	7	Tolerable
[E.15] Alteración de la información		60%	1	5	5	Tolerable
[E.16] Introducción de falsa información		50%	1	5	5	Tolerable
[E.17] Degradación de la información		60%	2	5	10	Moderado
[E.1] Errores de los usuarios		30%	2	3	6	Tolerable
[A.16] Introducción de falsa información		70%	1	6	6	Tolerable
	6	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		30%	3	2	6	Tolerable
[A.11] Acceso no autorizado		70%	1	4	4	Trivial
[A.14] Intercepción de información (escucha)		60%	1	4	4	Trivial
[A.19] Divulgación de información		80%	1	5	5	Tolerable
[D_P_Ofer]Plan de oferta educativa del centro	**10**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.15] Alteración de la información		50%	1	5	5	Tolerable
[E.16] Introducción de falsa información		50%	1	5	5	Tolerable
[E.17] Degradación de la información		60%	2	6	12	Moderado
[A.15] Modificación de información		70%	1	7	7	Tolerable
[A.16] Introducción de falsa información		50%	1	5	5	Tolerable

[D_OyF] Oferta educativa y Formación ocupacional	**9**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		10%	2	1	2	Trivial
[E.15] Alteración de la información		50%	1	5	5	Tolerable
[E.16] Introducción de falsa información		50%	1	5	5	Tolerable
[E.17] Degradación de la información		60%	2	5	10	Moderado
[A.15] Modificación de información		70%	1	6	6	Tolerable
[A.16] Introducción de falsa información		50%	1	5	5	Tolerable
[D_E_Alum_C]Evaluaciones definitivas de alumnos Participantes en cursos especiales.	**4**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		70%	3	3	9	Moderado
[E.15] Alteración de la información		50%	2	2	4	Trivial
[E.16] Introducción de falsa información		50%	1	2	2	Trivial
[E.17] Degradación de la información		60%	1	2	2	Trivial
[A.15] Modificación de información		30%	1	1	1	Trivial
[E.18] Destrucción de la información		70%	1	3	3	Trivial
[A.16] Introducción de falsa información		70%	1	3	3	Trivial
	6	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		30%	3	2	5	Tolerable
[A.11] Acceso no autorizado		70%	1	4	4	Trivial
[A.14] Intercepción de información (escucha)		60%	1	4	4	Trivial
[A.19] Divulgación de información		80%	1	5	5	Tolerable
[D_E_Alum_M]Evaluaciones definitivas de alumnos por módulos o bloque modular.	**4**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		50%	2	2	4	Trivial
[E.15] Alteración de la información		50%	1	2	2	Trivial
[E.16] Introducción de falsa información		50%	1	2	2	Trivial
[E.17] Degradación de la información		60%	1	2	2	Trivial
[A.11] Acceso no autorizado		30%	1	1	1	Trivial
[A.15] Modificación de información		70%	1	3	3	Trivial

[E.18] Destrucción de la información		70%	1	3	3	Trivial
	6	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		50%	3	3	9	Moderado
[A.11] Acceso no autorizado		70%	1	4	4	Trivial
[A.14] Intercepción de información (escucha)		60%	1	4	4	Trivial
[A.19] Divulgación de información		80%	1	5	5	Tolerable
[D_L_Alum]Listado de alumnos aspirantes	**6**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[A.15] Modificación de información		70%	1	4	4	Trivial
[E.15] Alteración de la información		50%	1	3	3	Trivial
[E.16] Introducción de falsa información		50%	1	3	3	Trivial
[E.17] Degradación de la información		60%	2	4	8	Tolerable
[E.1] Errores de los usuarios		30%	2	2	4	Trivial
[E.18] Destrucción de la información		70%	1	6	6	Tolerable
[A.16] Introducción de falsa información		70%	1	6	6	Tolerable
[D_L_Exa]Listado de examen	**5**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[A.15] Modificación de información		70%	1	4	4	Trivial
[E.15] Alteración de la información		60%	1	3	3	Trivial
[E.16] Introducción de falsa información		50%	1	3	3	Trivial
[E.17] Degradación de la información		60%	2	3	6	Tolerable
[E.1] Errores de los usuarios		30%	2	2	4	Trivial
[A.16] Introducción de falsa información		70%	1	4	4	Trivial
	7	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		70%	3	5	15	Importante
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.14] Intercepción de información (escucha)		60%	1	4	4	Trivial
[A.19] Divulgación de información		80%	1	6	6	Tolerable

[D_F_Eva]Formatos de evaluación de aprendizaje	**6**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[A.15] Modificación de información		70%	1	4	4	Trivial
[E.15] Alteración de la información		60%	1	4	4	Trivial
[E.16] Introducción de falsa información		50%	1	3	3	Trivial
[E.17] Degradación de la información		60%	2	4	8	Tolerable
[E.1] Errores de los usuarios		30%	2	2	4	Trivial
[A.16] Introducción de falsa información		70%	1	4	4	Trivial
	7	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		30%	3	2	6	Tolerable
[A.11] Acceso no autorizado		30%	1	2	2	Trivial
[A.14] Intercepción de información (escucha)		20%	1	1	1	Trivial
[A.19] Divulgación de información		40%	1	3	3	Trivial
[D_J_R] Jóvenes rurales e institutos	**9**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[A.15] Modificación de información		90%	1	8	8	Tolerable
[E.15] Alteración de la información		60%	1	5	5	Tolerable
[E.16] Introducción de falsa información		50%	1	5	5	Tolerable
[E.17] Degradación de la información		60%	2	5	10	Moderado
[E.1] Errores de los usuarios		30%	3	3	9	Moderado
[A.16] Introducción de falsa información		90%	1	8	8	Tolerable
[E.18] Destrucción de la información		70%	1	6	6	Tolerable
[D_R] reservado	**10**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		30%	4	3	12	Moderado
[E.2] Errores del administrador		60%	3	6	18	Intolerable
[E.15] Alteración de la información		60%	1	6	6	Tolerable
[E.16] Introducción de falsa información		60%	1	6	6	Tolerable
[E.17] Degradación de la información		80%	1	8	8	Tolerable
[A.11] Acceso no autorizado		75%	1	8	8	Tolerable
[A.15] Modificación de información		75%	1	8	8	Tolerable

[E.18] Destrucción de la información		70%	1	7	7	Tolerable
[E.18] Destrucción de la información		70%	1	7	7	Tolerable
	7	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		85%	1	6	6	Tolerable
[A.11] Acceso no autorizado		90%	1	6	6	Tolerable
[A.14] Intercepción de información (escucha)		90%	1	6	6	Tolerable
[A.19] Divulgación de información		95%	1	7	7	Tolerable
	10	**[A_D]**	**Fre**	**Impac**	**Riesgo**	
[E.2] Errores del administrador		80%	1	8	8	Tolerable
[D_C] confidencial	**3**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		30%	1	1	1	Trivial
[E.15] Alteración de la información		50%	1	2	2	Trivial
[E.16] Introducción de falsa información		50%	1	2	2	Trivial
[E.17] Degradación de la información		50%	1	2	2	Trivial
[A.11] Acceso no autorizado		60%	1	2	2	Trivial
[A.15] Modificación de información		60%	1	2	2	Trivial
[E.18] Destrucción de la información		70%	1	2	2	Trivial
	9	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		60%	2	5	10	Moderado
[A.11] Acceso no autorizado		70%	1	6	6	Tolerable
[A.14] Intercepción de información (escucha)		60%	1	5	5	Tolerable
[A.19] Divulgación de información		50%	1	5	5	Tolerable
[D_SC] datos sin clasificar	**5**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		30%	1	2	2	Trivial
[E.15] Alteración de la información		40%	2	2	4	Trivial
[E.16] Introducción de falsa información		40%	2	2	4	Trivial
[E.17] Degradación de la información		30%	1	2	2	Trivial

[A.11] Acceso no autorizado		30%	1	2	2	Trivial
[A.15] Modificación de información		30%	1	2	2	Trivial
[E.18] Destrucción de la información		70%	1	4	4	Trivial
	5	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		50%	2	3	6	Tolerable
[A.11] Acceso no autorizado		50%	1	3	3	Trivial
[A.14] Intercepción de información (escucha)		50%	1	3	3	Trivial
[A.19] Divulgación de información		50%	1	3	3	Trivial
[D_Ins_p]Datos instructores.	**6**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		60%	1	4	4	Trivial
[E.15] Alteración de la información		60%	1	4	4	Trivial
[E.16] Introducción de falsa información		70%	1	4	4	Trivial
[E.17] Degradación de la información		80%	1	5	5	Tolerable
[A.11] Acceso no autorizado		70%	1	4	4	Trivial
[A.15] Modificación de información		75%	1	5	5	Tolerable
[E.18] Destrucción de la información		70%	1	4	4	Trivial
	6	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		60%	1	4	4	Trivial
[A.11] Acceso no autorizado		65%	1	4	4	Trivial
[A.14] Intercepción de información (escucha)		60%	1	4	4	Trivial
[A.19] Divulgación de información		30%	1	2	2	Trivial
[D_P_plan]Datos del personal de planta.	**6**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		50%	1	3	3	Trivial
[E.15] Alteración de la información		80%	1	5	5	Tolerable
[E.16] Introducción de falsa información		80%	1	5	5	Tolerable
[E.17] Degradación de la información		70%	1	4	4	Trivial
[A.11] Acceso no autorizado		60%	1	4	4	Trivial
[E.18] Destrucción de la información		70%	1	4	4	Trivial

	6	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		60%	1	4	4	Trivial
[A.11] Acceso no autorizado		70%	1	4	4	Trivial
[A.14] Intercepción de información (escucha)		60%	1	4	4	Trivial
[A.19] Divulgación de información		70%	1	4	4	Trivial
[D_Com]Ordenes de compra	**7**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		50%	1	4	4	Trivial
[E.15] Alteración de la información		80%	1	6	6	Tolerable
[E.16] Introducción de falsa información		80%	1	6	6	Tolerable
[E.17] Degradación de la información		70%	1	5	5	Tolerable
[A.11] Acceso no autorizado		60%	1	4	4	Trivial
[E.18] Destrucción de la información		70%	1	5	5	Tolerable
	7	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		60%	2	4	8	Tolerable
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.14] Intercepción de información (escucha)		60%	1	4	4	Trivial
[A.19] Divulgación de información		70%	1	5	5	Tolerable
[D_Cot]listado de cotizaciones	**7**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		70%	1	5	5	Tolerable
[E.15] Alteración de la información		80%	1	6	6	Tolerable
[E.16] Introducción de falsa información		90%	1	6	6	Tolerable
[E.17] Degradación de la información		75%	1	5	5	Tolerable
[E.18] Destrucción de la información		70%	1	5	5	Tolerable
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.15] Modificación de información		90%	1	6	6	Tolerable
[A.16] Introducción de falsa información		80%	1	6	6	Tolerable
	7	**[C]**	**Fre**	**Impac**	**Riesgo**	
[E.19] Divulgación de información		60%	2	4	8	Tolerable

[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.14] Intercepción de información (escucha)		60%	1	4	4	Trivial
[A.19] Divulgación de información		70%	1	5	5	Tolerable
[D_Pres]Solicitud presupuestal	**7**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		40%	3	3	9	Moderado
[E.15] Alteración de la información		80%	1	6	6	Tolerable
[E.16] Introducción de falsa información		90%	1	6	6	Tolerable
[E.17] Degradación de la información		75%	1	5	5	Tolerable
[E.18] Destrucción de la información		70%	1	5	5	Tolerable
[A.11] Acceso no autorizado		80%	1	6	6	Tolerable
[A.15] Modificación de información		90%	1	6	6	Tolerable
[A.16] Introducción de falsa información		80%	1	6	6	Tolerable
[A.17] Corrupción de la información		90%	1	6	6	Tolerable
	7	**[C]**	**Fre**	**Impacto**	**Riesgo**	
[E.19] Divulgación de información		60%	2	4	8	Tolerable
[A.11] Acceso no autorizado		70%	1	5	5	Tolerable
[A.14] Intercepción de información (escucha)		60%	1	4	4	Trivial
[A.19] Divulgación de información		70%	1	5	5	Tolerable
[D_Apr]Información sobre aprendices TIC SOLUTION	**6**	**[I]**	**Fre**	**Impac**	**Riesgo**	
[E.1] Errores de los usuarios		60%	2	4	8	Tolerable
[E.15] Alteración de la información		60%	1	4	4	Trivial
[E.16] Introducción de falsa información		70%	1	4	4	Trivial
[E.17] Degradación de la información		80%	2	5	10	Moderado
[A.11] Acceso no autorizado		70%	1	4	4	Trivial
[A.15] Modificación de información		75%	1	5	5	Tolerable
[A.16] Introducción de falsa información		70%	1	4	4	Trivial
	6	**[C]**	**Fre**	**Impac**	**Riesgo**	

[E.19] Divulgación de información		60%	2	4	8	Tolerable
[A.11] Acceso no autorizado		70%	1	4	4	Trivial
[A.14] Intercepción de información (escucha)		60%	1	4	4	Trivial
[A.19] Divulgación de información		70%	1	4	4	Trivial

Personal

ACTIVOS/AMENAZAS	Valor	Dimen				
[ui] Usuarios Internos	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riesgo**
[E.28] Indisponibilidad del personal.		60%	1	4	4	Trivial
[A.28] Indisponibilidad del personal.		80%	1	6	6	Tolerable
[P-Adm] Administradores de Sistemas	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.28] Indisponibilidad del personal.		60%	1	5	5	Tolerable
[A.28] Indisponibilidad del personal.		80%	1	7	7	Tolerable
[P-Com] Administradores de Comunicaciones	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.28] Indisponibilidad del personal.		60%	1	5	5	Tolerable
[A.28] Indisponibilidad del personal.		80%	1	7	7	Tolerable
[P-DBa] Administradores de Bases de Datos	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.28] Indisponibilidad del personal.		60%	1	5	5	Tolerable
[A.28] Indisponibilidad del personal.		80%	1	7	7	Tolerable
[P-Desrr] Desarrolladores	**3**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.28] Indisponibilidad del personal.		60%	1	2	2	Trivial
[A.28] Indisponibilidad del personal.		80%	1	2	2	Trivial
[P_C_Acd] Coordinador académico	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.28] Indisponibilidad del personal.		60%	1	5	5	Tolerable

[A.28] Indisponibilidad del personal.		80%	1	7	7	Tolerable
[P_SDir] Subdirector de Centro	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.28] Indisponibilidad del personal.		60%	1	7	7	Tolerable
[A.28] Indisponibilidad del personal.		80%	1	7	7	Tolerable
[P_C_Pro] Coordinadora de formación profesional	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.28] Indisponibilidad del personal.		60%	1	5	5	Tolerable
[A.28] Indisponibilidad del personal.		80%	1	7	7	Tolerable
[P_C_admin] Coordinador Administrativo	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.28] Indisponibilidad del personal.		60%	1	5	5	Tolerable
[A.28] Indisponibilidad del personal.		80%	1	7	7	Tolerable
[P_C_TH] Talento Humano	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.28] Indisponibilidad del personal.		60%	1	4	4	Trivial
[A.28] Indisponibilidad del personal.		80%	1	6	6	Tolerable
[ue] Usuarios externos	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[E.28] Indisponibilidad del personal.		60%	1	4	4	Trivial
[A.28] Indisponibilidad del personal.		80%	1	6	6	Tolerable

Instalaciones

ACTIVOS/AMENAZAS	Valor	Dimen				
[building]Edificio	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[N.1] Fuego		90%	1	8	8	Tolerable
[N.2] Daños por agua		70%	1	6	6	Tolerable
[N.*] Desastres naturales		80%	1	7	7	Tolerable
[I.1] Fuego		80%	1	7	7	Tolerable
[I.2] Daños por agua		70%	1	6	6	Tolerable
[I.*] Desastres industriales		80%	1	7	7	Tolerable

Soportes De Información

ACTIVOS/AMENAZAS	Valor	Dimen				
[CD] Cd-Rom	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riesgo**
[N.1] Fuego		90%	1	6	6	Tolerable
[N.2] Daños por agua		10%	1	1	1	Trivial
[N.*] Desastres naturales		30%	1	2	2	Trivial
[I.1] Fuego		90%	1	6	6	Tolerable
[N.1] Fuego		90%	1	6	6	Tolerable
[I.2] Daños por agua		10%	1	1	1	Trivial
[I.*] Desastres industriales		10%	1	1	1	Trivial
[I.10] Degradación de los soportes de almacenamiento de la información.		70%	2	5	10	Moderado
[A.25] Robo		100%	1	7	7	Tolerable
[I.5] Avería de origen físico o lógico		50%	2	4	8	Tolerable

[usb]Dispositivos USB	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riesgo**
[N.1] Fuego		90%	1	6	6	Tolerable
[N.2] Daños por agua		50%	1	4	4	Trivial
[N.*] Desastres naturales		30%	1	2	2	Trivial
[I.1] Fuego		90%	1	6	6	Tolerable
[I.2] Daños por agua		50%	1	4	4	Trivial
[I.*] Desastres industriales		50%	1	4	4	Trivial
[I.5] Avería de origen físico o lógico		50%	2	4	8	Tolerable
[I.10] Degradación de los soportes de almacenamiento de la información.		60%	2	4	8	Tolerable
[A.25] Robo		100%	1	7	7	Tolerable
[tape] Cinta Magnética	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riesgo**
[N.1] Fuego		90%	1	6	6	Tolerable
[N.2] Daños por agua		10%	1	1	1	Trivial
[N.*] Desastres naturales		30%	1	2	2	Trivial
[I.1] Fuego		90%	1	6	6	Tolerable
[I.2] Daños por agua		10%	1	1	1	Trivial
[I.*] Desastres industriales		10%	1	1	1	Trivial
[I.10] Degradación de los soportes de almacenamiento de la información.		70%	2	5	10	Moderado
[A.25] Robo		100%	1	7	7	Tolerable
[I.5] Avería de origen físico o lógico		50%	2	4	8	Tolerable
[Disk] Discos Duros	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riesgo**
[N.1] Fuego		90%	1	6	6	Tolerable
[N.2] Daños por agua		50%	1	4	4	Trivial
[N.*] Desastres naturales		30%	1	2	2	Trivial
[I.1] Fuego		90%	1	6	6	Tolerable
[I.2] Daños por agua		50%	1	4	4	Trivial
[I.*] Desastres industriales		50%	1	4	4	Trivial

[I.5] Avería de origen físico o lógico		50%	2	4	7	Tolerable
[I.10] Degradación de los soportes de almacenamiento de la información.		60%	2	4	8	Tolerable
[A.25] Robo		100%	1	7	7	Tolerable
[printed] Material Impreso	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riesgo**
[N.1] Fuego		100%	1	7	7	Tolerable
[N.2] Daños por agua		70%	1	5	5	Tolerable
[N.*] Desastres naturales		50%	1	4	4	Trivial
[I.1] Fuego		100%	1	7	7	Tolerable
[I.2] Daños por agua		50%	1	4	4	Trivial
[I.*] Desastres industriales		50%	1	4	4	Trivial
[I.10] Degradación de los soportes de almacenamiento de la información.		50%	2	4	8	Tolerable
[A.11] Acceso no autorizado		40%	1	3	3	Trivial
[A.25] Robo		100%	1	7	7	Tolerable
[I.5] Avería de origen físico o lógico		50%	2	4	8	Tolerable

Equipamiento Auxiliar

ACTIVOS/AMENAZAS	**Valor**	**Dimen**				
[AUX _ups] Sistemas de Alimentación Interrumpida	**5**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[N.1] Fuego		80%	1	4	4	Trivial
[N.2] Daños por agua		80%	1	4	4	Trivial
[N.*] Desastres naturales		70%	1	4	4	Trivial
[I.1] Fuego		80%	1	4	4	Trivial
[I.2] Daños por agua		80%	1	4	4	Trivial
[I.*] Desastres industriales		80%	1	4	4	Trivial
[I.5] Avería de origen físico o lógico		80%	2	4	8	Tolerable

[I.6] Corte del suministro eléctrico		70%	2	4	8	Tolerable
[I.7] Condiciones inadecuadas de temperatura y/o Humedad		50%	1	3	3	Trivial
[A.25] Robo		80%	1	4	4	Trivial
[AUX _gen] Generadores Eléctricos	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[N.1] Fuego		70%	1	5	5	Tolerable
[N.2] Daños por agua		70%	1	5	5	Tolerable
[N.*] Desastres naturales		80%	1	6	6	Tolerable
[I.1] Fuego		70%	1	5	5	Tolerable
[I.2] Daños por agua		80%	1	6	6	Tolerable
[I.*] Desastres industriales		80%	1	6	6	Tolerable
[I.5] Avería de origen físico o lógico		70%	1	5	5	Tolerable
[I.6] Corte del suministro eléctrico		70%	2	5	10	Moderado
[I.7] Condiciones inadecuadas de temperatura y/o Humedad		60%	2	4	8	Tolerable
[A.25] Robo		80%	1	6	6	Tolerable
[AUX _ac] Equipos de Climatización	**5**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[N.1] Fuego		70%	1	4	4	Trivial
[N.2] Daños por agua		80%	1	4	4	Trivial
[N.*] Desastres naturales		70%	1	4	4	Trivial
[I.1] Fuego		70%	1	4	4	Trivial
[I.2] Daños por agua		60%	1	3	3	Trivial
[I.*] Desastres industriales		80%	1	4	4	Trivial
[I.5] Avería de origen físico o lógico		60%	1	3	3	Trivial
[I.6] Corte del suministro eléctrico		70%	2	4	8	Tolerable
[A.7] Uso no previsto		30%	2	2	4	Trivial
[A.25] Robo		70%	1	4	4	Trivial
[AUX _cabling] Cableado	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**

[N.1] Fuego		70%	1	5	5	Tolerable
[N.2] Daños por agua		60%	1	4	4	Trivial
[N.*] Desastres naturales		70%	1	5	5	Tolerable
[I.1] Fuego		60%	1	4	4	Trivial
[I.2] Daños por agua		70%	1	5	5	Tolerable
[I.*] Desastres industriales		80%	1	6	6	Tolerable
[I.5] Avería de origen físico o lógico		50%	2	4	8	Tolerable
[I.7] Condiciones inadecuadas de temperatura y/o Humedad		50%	2	4	8	Tolerable
[A.25] Robo		70%	1	5	5	Tolerable
[AUX _armario]armario archivador	**1**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riego**
[N.1] Fuego		70%	1	1	1	Trivial
[N.2] Daños por agua		80%	1	1	1	Trivial
[N.*] Desastres naturales		70%	1	1	1	Trivial
[I.2] Daños por agua		70%	1	1	1	Trivial
[I.*] Desastres industriales		80%	1	1	1	Trivial
[I.5] Avería de origen físico o lógico		70%	2	1	2	Trivial
[I.7] Condiciones inadecuadas de temperatura y/o Humedad		50%	2	1	2	Trivial
[A.25] Robo		70%	1	1	1	Trivial

Comunicaciones

ACTIVOS/AMENAZAS	**Valor**	**Dimen**				
[COM_PSTN] Red Telefónica	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	**Tipo riesgo**
[N.1] Fuego		80%	1	6	6	Tolerable
[N.2] Daños por agua		60%	1	4	4	Trivial
[N.*] Desastres naturales		80%	1	6	6	Tolerable

[I.2] Daños por agua		60%	1	4	4	Trivial
[I.5] Avería de origen físico o lógico		60%	2	4	8	Tolerable
[E.2] Errores del administrador		70%	1	5	5	Tolerable
[E.24] Caída del sistema por agotamiento de recursos		70%	1	5	5	Tolerable
[A.25] Robo		80%	1	6	6	Tolerable
[COM_radio] Red Inalámbrica	**7**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[N.1] Fuego		80%	1	6	6	Tolerable
[N.*] Desastres naturales		80%	1	6	6	Tolerable
[I.2] Daños por agua		70%	1	5	5	Tolerable
[I.2] Daños por agua		70%	1	5	5	Tolerable
[I.*] Desastres industriales		80%	1	6	6	Tolerable
[I.5] Avería de origen físico o lógico		70%	2	5	10	Moderado
[I.6] Corte del suministro eléctrico		80%	2	6	12	Moderado
[I.7] Condiciones inadecuadas de temperatura y/o humedad		50%	2	4	8	Tolerable
[E.2] Errores del administrador		70%	1	5	5	Tolerable
[E.4] Errores de configuración		80%	1	6	6	Tolerable
[E.24] Caída del sistema por agotamiento de recursos		70%	1	5	5	Tolerable
[A.24] Denegación de servicio		100%	1	7	7	Tolerable
[A.25] Robo		80%	1	6	6	Tolerable
[COM_micro] Microondas	**5**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[N.1] Fuego		80%	1	4	4	Trivial
[N.2] Daños por agua		70%	1	4	4	Trivial
[N.*] Desastres naturales		80%	1	4	4	Trivial
[I.2] Daños por agua		70%	1	4	4	Trivial
[I.*] Desastres industriales		80%	1	4	4	Trivial

[I.5] Avería de origen físico o lógico		70%	2	4	8	Tolerable
[I.6] Corte del suministro eléctrico		80%	2	4	8	Tolerable
[I.7] Condiciones inadecuadas de temperatura y/o humedad		50%	2	3	6	Tolerable
[E.2] Errores del administrador		70%	1	4	4	Trivial
[E.4] Errores de configuración		80%	1	4	4	Trivial
[E.24] Caída del sistema por agotamiento de recursos		70%	1	4	4	Trivial
[A.25] Robo		90%	1	5	5	Tolerable
[COM_Red] Red	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[N.1] Fuego		80%	1	7	7	Tolerable
[N.2] Daños por agua		70%	1	6	6	Tolerable
[N.*] Desastres naturales		80%	1	7	7	Tolerable
[I.2] Daños por agua		80%	1	7	7	Tolerable
[I.*] Desastres industriales		80%	1	7	7	Tolerable
[I.5] Avería de origen físico o lógico		70%	2	6	12	Moderado
[I.6] Corte del suministro eléctrico		70%	2	6	12	Moderado
[I.7] Condiciones inadecuadas de temperatura y/o humedad		50%	2	5	10	Moderado
[E.2] Errores del administrador		70%	1	6	6	Tolerable
[E.4] Errores de configuración		80%	1	7	7	Tolerable
[E.24] Caída del sistema por agotamiento de recursos		70%	1	6	6	Tolerable
[A.24] Denegación de servicio		100%	1	9	9	Moderado
[A.25] Robo		80%	1	7	7	Tolerable

Equipos Informáticos

ACTIVOS/AMENAZAS	Valor	Dimen				
[HW_S] servidores	**9**	**[D]**	**Fre**	**Impac**	**Riesgo**	
[N.*] Desastres naturales		80%	1	7	7	Tolerable
[N.2] Daños por agua		80%	1	7	7	Tolerable
[N.1] Fuego		80%	1	7	7	Tolerable
[I.2] Daños por agua		80%	1	7	7	Tolerable
[I.5] Avería de origen físico o lógico		60%	2	5	10	Moderado
[I.6] Corte del suministro eléctrico		70%	2	6	12	Moderado
[I.7] Condiciones inadecuadas de temperatura y/o humedad		50%	2	5	10	Moderado
[A.4] Manipulación de la configuración		80%	1	7	7	Tolerable
[A.24] Denegación de servicio		100%	1	9	9	Moderado
[A.25] Robo		100%	1	9	9	Moderado
[E.2] Errores del administrador		70%	1	6	6	Tolerable
[HW_PC] informática personal	2	**[D]**	**Fre**	**Impac**	**Riesgo**	
[N.*] Desastres naturales		80%	1	2	2	Trivial
[N.2] Daños por agua		80%	1	2	2	Trivial
[N.1] Fuego		80%	1	2	2	Trivial
[I.2] Daños por agua		80%	1	2	2	Trivial
[I.5] Avería de origen físico o lógico		60%	2	1	2	Trivial
[I.6] Corte del suministro eléctrico		70%	2	1	3	Trivial
[I.7] Condiciones inadecuadas de temperatura y/o humedad		50%	2	1	2	Trivial
[A.4] Manipulación de la configuración		80%	1	2	2	Trivial
[A.24] Denegación de servicio		100%	1	2	2	Trivial
[A.25] Robo		100%	1	2	2	Trivial

[E.2] Errores del administrador		70%	1	1	1	Trivial
[HW_PRINT] medios de impresión	2	**[D]**	**Fre**	**Impac**	**Riesgo**	
[N.*] Desastres naturales		80%	1	2	2	Trivial
[N.2] Daños por agua		80%	1	2	2	Trivial
[N.1] Fuego		80%	1	2	2	Trivial
[I.2] Daños por agua		80%	1	2	2	Trivial
[I.5] Avería de origen físico o lógico		60%	2	1	2	Trivial
[I.6] Corte del suministro eléctrico		70%	2	1	3	Trivial
[I.7] Condiciones inadecuadas de temperatura y/o humedad		50%	2	1	2	Trivial
[A.4] Manipulación de la configuración		80%	1	2	2	Trivial
[A.24] Denegación de servicio		100%	1	2	2	Trivial
[A.25] Robo		100%	1	2	2	Trivial
[E.2] Errores del administrador		70%	1	1	1	Trivial
[HW_switch] conmutadores	5	**[D]**	**Fre**	**Impac**	**Riesgo**	
[N.*] Desastres naturales		80%	1	4	4	Trivial
[N.2] Daños por agua		80%	1	4	4	Trivial
[N.1] Fuego		80%	1	4	4	Trivial
[I.2] Daños por agua		80%	1	4	4	Trivial
[I.5] Avería de origen físico o lógico		60%	2	3	6	Tolerable
[I.6] Corte del suministro eléctrico		70%	2	4	8	Tolerable
[I.7] Condiciones inadecuadas de temperatura y/o humedad		50%	2	3	6	Tolerable
[A.4] Manipulación de la configuración		80%	1	4	4	Trivial
[A.24] Denegación de servicio		100%	1	5	5	Tolerable
[A.25] Robo		100%	1	5	5	Tolerable
[E.2] Errores del administrador		70%	1	4	4	Trivial
[HW_router] encaminadores	5	**[D]**	**Fre**	**Impac**	**Riesgo**	

[N.*] Desastres naturales		80%	1	4	4	Trivial
[N.2] Daños por agua		80%	1	4	4	Trivial
[N.1] Fuego		80%	1	4	4	Trivial
[I.2] Daños por agua		80%	1	4	4	Trivial
[I.5] Avería de origen físico o lógico		60%	2	3	6	Tolerable
[I.6] Corte del suministro eléctrico		70%	2	4	8	Tolerable
[I.7] Condiciones inadecuadas de temperatura y/o humedad		50%	2	3	6	Tolerable
[A.4] Manipulación de la configuración		80%	1	4	4	Trivial
[A.24] Denegación de servicio		100%	1	5	5	Tolerable
[A.25] Robo		100%	1	5	5	Tolerable
[E.2] Errores del administrador		70%	1	4	4	Trivial
[HW_Cons] Consola de Descarga y video conferencia	3	**[D]**	**Fre**	**Impac**	**Riesgo**	
[N.*] Desastres naturales		80%	1	2	2	Trivial
[N.2] Daños por agua		80%	1	2	2	Trivial
[N.1] Fuego		80%	1	2	2	Trivial
[I.2] Daños por agua		80%	1	2	2	Trivial
[I.5] Avería de origen físico o lógico		60%	2	2	4	Trivial
[I.6] Corte del suministro eléctrico		70%	2	2	4	Trivial
[I.7] Condiciones inadecuadas de temperatura y/o humedad		50%	2	2	4	Trivial
[A.4] Manipulación de la configuración		80%	1	2	2	Trivial
[A.24] Denegación de servicio		100%	1	3	3	Trivial
[A.25] Robo		100%	1	3	3	Trivial
[E.2] Errores del administrador		70%	1	2	2	Trivial
[HW_Acces] Access point	3	**[D]**	**Fre**	**Impac**	**Riesgo**	
[N.*] Desastres naturales		80%	1	2	2	Trivial
[N.2] Daños por agua		80%	1	2	2	Trivial

[N.1] Fuego		80%	1	2	2	Trivial
[I.2] Daños por agua		80%	1	2	2	Trivial
[I.5] Avería de origen físico o lógico		60%	2	2	4	Trivial
[I.6] Corte del suministro eléctrico		70%	2	2	4	Trivial
[I.7] Condiciones inadecuadas de temperatura y/o humedad		50%	2	2	4	Trivial
[A.4] Manipulación de la configuración		80%	1	2	2	Trivial
[A.24] Denegación de servicio		100%	1	3	3	Trivial
[A.25] Robo		100%	1	3	3	Trivial
[E.2] Errores del administrador		70%	1	2	2	Trivial
[HW_Escan] Scanner	2	**[D]**	**Fre**	**Impac**	**Riesgo**	
[N.*] Desastres naturales		80%	1	2	2	Trivial
[N.2] Daños por agua		80%	1	2	2	Trivial
[N.1] Fuego		80%	1	2	2	Trivial
[I.2] Daños por agua		80%	1	2	2	Trivial
[I.5] Avería de origen físico o lógico		60%	2	1	2	Trivial
[I.6] Corte del suministro eléctrico		70%	2	1	2	Trivial
[I.7] Condiciones inadecuadas de temperatura y/o humedad		50%	2	1	2	Trivial
[A.4] Manipulación de la configuración		80%	1	2	2	Trivial
[A.24] Denegación de servicio		100%	1	2	2	Trivial
[A.25] Robo		100%	1	2	2	Trivial
[E.2] Errores del administrador		70%	1	1	1	Trivial

RIESGO ACEPTADO

De acuerdo a los objetivos trazados por la dirección de la institución, se define que el nivel de riesgo aceptado por la institución es aquel que este dentro del rango TRIVIAL a MODERADO a partir de ello se toma como referencia para aplicar controles y formular proyectos que permitan reducir el nivel de riesgo al cual está expuesta la institución ante una eventual amenaza.

Tipos de riesgo	Rango
Trivial	[0- 4]
Tolerable	[5- 8]
Moderado	[9 – 13]

11. PLAN DE TRATAMIENTO DE RIESGOS

A continuación se detallaran las medidas de protección y salvaguardas que se implementaran para la relación activo/amenaza/política en la institución.

APLICACIONES

Amenaza: [E.8] Difusión de software dañino y [A.8] Difusión de software dañino.

1. En todos los equipos de la empresa debe existir una herramienta antivirus ejecutándose permanentemente y en continua actualización para examinar todo software que venga de afuera o inclusive de otros departamentos de la compañía. Se establecerán normas de mantenimiento y aviso ante posibles infecciones, de forma que el usuario sepa en todo momento a quién debe y cómo debe comunicar una posible infección por virus.

2. Se establecerán las normas y medidas adecuadas para detectar cualquier intento de ataque a la red tanto desde el exterior como desde el interior.

3. Esta estrictamente prohibido utilizar herramientas propias de delincuentes informáticos, tales como programas que rastrean vulnerabilidades en sistemas de cómputo propios u ajenos.

4. La empresa destinará los recursos necesarios para que exista un plan de formación continuado que garantice tanto los aspectos de seguridad de la información como la producción o cualquier elemento de seguridad inherente a la empresa.

5. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será

sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

6. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

7. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenazas: [A.4] Manipulación de la configuración [E.4] Errores de configuración.

1. Deben existir sistemas de control automatizados que le permitan al administrador conocer en cualquier momento los accesos al sistema por usuarios autorizados o no autorizados, así como también conocer las actividades realizadas durante los accesos a los programas. Además se debe controlar la instalación o desinstalación de programas licenciados o no.

2. Las configuraciones de cada uno de los dispositivos de interconexión de red, equipos de cómputo y aplicaciones deben ser almacenadas en manuales y en copias de seguridad.

3. Debe implantarse un sistema de autorización y control de acceso a los equipos de cómputos y redes, con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos o configuraciones importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

4. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

5. Deberán existir estándares de configuración de los puestos de trabajo, servidores y demás equipos de la red de la información. Con base al estándar se deberá generar un procedimiento donde se especifique qué aplicaciones deben instalarse

de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.

6. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

7. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [E.21] Errores de mantenimiento / actualización.

1. No se puede modificar la configuración de hardware y software, por personal no autorizado en caso contrario debe existir mecanismos de control adecuado.

2. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

3. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [E.20] Vulnerabilidades de los programas (software).

1. Los desarrollos de software deberán incluir un estudio de seguridad para establecer las medidas de seguridad normalizadas por la dirección de la empresa y en todo caso siempre tendrán la consideración de ser un bien propiedad de la misma.

2. Los administradores del sistema deberán buscar nuevas vulnerabilidades en los sistemas, estudiarlas, informarlas a la dirección general, y minimizar los riesgos de dicha amenaza para luego documentarla.

3. Esta estrictamente prohibido utilizar herramientas propias de delincuentes informáticos, tales como programas que rastrean vulnerabilidades en sistemas de computo propios u ajenos.

4. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

5. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

6. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [A.5] Suplantación de la identidad del usuario.

1. Cualquier usuario deberá ser identificado por los medios apropiados para poder acceder a los recursos de red o a las aplicaciones.

2. Se establecerán las medidas y normas oportunas para restringir los accesos a las zonas previamente establecidas, de forma que sólo se pueda acceder a los recursos asignados.

3. Las cuentas deberán ser otorgadas por el departamento de sistemas a usuarios legítimos, además las contraseñas elegidas por lo usuarios deberán ser seguras, de tal forma que no se utilicen datos personales, alias, secuencia de caracteres conocida o palabras predecibles en las contraseñas.

4. Esta prohibido acceder al sistema con una cuenta diferente a la propia, aun con la autorización del dueño de dicha cuenta.

5. No abandonar el equipo sin antes haber cerrado la sesión o el programa.

6. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

7. Los empleados que actualmente no se encuentran vinculados con la institución se les aplicara un procedimiento de baja de todas las cuentas de usuarios y privilegios de acceso.

8. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

9. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [A.11] Acceso no autorizado.

1. Se establecerán las medidas y normas oportunas para restringir los accesos a las zonas previamente establecidas, de forma que sólo se pueda acceder a los recursos asignados aquellos que sean autorizados y tengan esos privilegios.

2. Debe existir procedimientos o sistemas de control automatizados que le permitan al administrador conocer en cualquier momento los accesos al sistema por usuarios autorizados o no.

3. Debe existir sistema de control que permitan al administrador de la planta o espacio físico conocer el acceso a las áreas críticas por personal no autorizado.

4. El acceso del personal autorizado de procesamiento así como el personal contratado sólo podrá permanecer en las instalaciones de las empresas durante el horario autorizado.

5. Los empleados que actualmente no se encuentran vinculados con la institución se les aplicara un procedimiento de baja de todas las cuentas de usuarios y privilegios de acceso.

6. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

7. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

8. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

SERVICIOS

Amenaza: [E.24] Caída del sistema por agotamiento de recursos.

1. La institución deberá contar con mecanismos de recuperación y tolerantes a fallos del sistema.

2. Los dispositivos de nertworking, equipos de cómputo y la red del centro de Tic Solution deben contar y cumplir con especificaciones y estándares necesarios para brindar una buena calidad de servicio.

3. Se deberá documentar en planos los canales de tendidos de cables y la estructura de la red general.

4. Cualquier difusión, eliminación, destrucción, modificación ó interrupción que afecte a la disponibilidad, integridad, confidencialidad o autenticidad de la información, así como

a los medios de tratamiento ó comunicación de la misma, será atendido de inmediato con procedimientos ante respuesta de incidentes además este será documentado.

5. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

6. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [E.1] Errores de los usuarios

1. Debe existir capacitación u orientación a los usuarios que utilizan cada uno de los servicios pertenecientes a la institución.

2. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

3. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos

Amenaza: [A.24] Denegación de servicio

1. La ubicación del tendido del cableado y los equipos de red o equipos críticos de la institución tienen que estar lejos del alcance de personal no autorizado.

2. La institución deberá contar con mecanismos de recuperación y tolerantes a fallos del sistema.

3. Cualquier cambio que se desee realizar en el plano general de la ubicación de los equipos, debe ser previamente autorizado y aprobado por el administrador de sistemas.

4. Los dispositivos de networking, equipos de cómputo y la red del centro de Tic Solution deben contar y cumplir con especificaciones y estándares necesarios para brindar una buena calidad de servicio.

5. Esta estrictamente prohibido utilizar herramientas propias de delincuentes informáticos, tales como programas que rastrean vulnerabilidades en sistemas de cómputo propios u ajenos.

6. Cualquier difusión, eliminación, destrucción, modificación ó interrupción que afecte a la disponibilidad, integridad, confidencialidad o autenticidad de la información, así como a los medios de tratamiento ó comunicación de la misma, será atendido de inmediato con procedimientos ante respuesta de incidentes además este será documentado.

7. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

8. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

9. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

10. Esta estrictamente prohibido utilizar herramientas propias de delincuentes informáticos, tales como programas que rastrean vulnerabilidades en sistemas de computo propios u ajenos.

Amenazas: [A.4] Manipulación de la configuración [E.4] Errores de configuración.
A.10.9.3

1. Deben existir sistemas de control automatizados que le permitan al administrador conocer en cualquier momento los accesos al sistema por usuarios autorizados o no autorizados, así como también conocer las actividades realizadas durante los accesos a los programas. Además se debe controlar la instalación o desinstalación de programas licenciados o no.

2. Las configuraciones de cada uno de los dispositivos de interconexión de red, equipos de cómputo y aplicaciones deben ser almacenadas en manuales y en copias de seguridad.

3. Debe implantarse un sistema de autorización y control de acceso a los equipos de cómputos y redes, con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos o configuraciones importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

4. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

5. Deberán existir estándares de configuración de los puestos de trabajo, servidores y demás equipos de la red de la información. Con base al estándar se deberá generar un procedimiento donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.

6. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

7. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos

Amenaza: [A.5] Suplantación de la identidad del usuario.

1. Cualquier usuario deberá ser identificado por los medios apropiados para poder acceder a los recursos de red o a las aplicaciones.

2. Se establecerán las medidas y normas oportunas para restringir los accesos a las zonas previamente establecidas, de forma que sólo se pueda acceder a los recursos asignados.

3. Las cuentas deberán ser otorgadas por el departamento de sistemas a usuarios legítimos, además las contraseñas elegidas por lo usuarios deberán ser seguras, de tal forma que no se utilicen datos personales, alias, secuencia de caracteres conocida o palabras predecibles en las contraseñas.

4. Esta prohibido acceder al sistema con una cuenta diferente a la propia, aun con la autorización del dueño de dicha cuenta.

5. No abandonar el equipo sin antes haber cerrado la sesión o el programa.

6. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

7. Los empleados que actualmente no se encuentran vinculados con la institución se les aplicara un procedimiento de baja de todas las cuentas de usuarios y privilegios de acceso.

8. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

9. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [E.2] Errores del administrador.

1. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y

manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

2. El Administrador del sistema se encargará de evaluar el incidente ó el error, trazar un plan de acción, llevarlo a cabo, comprobar los resultados y actuar en consecuencia.

3. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos

Amenaza: [A.7] Uso no previsto.

1. Las activos usados por los usuarios son provistos por la organización son de su propiedad o están debidamente licenciadas a su nombre. Su utilización será dedicada exclusivamente para efectos laborales, académicos, de investigación, de administración y de atención al cliente. Cualquier otro uso deberá ser consultado al administrador.

2. El administrador de los activos tecnológicos provistos por la institución asume responsabilidad directa por su uso apropiado y se compromete a cumplir con las políticas establecidas en el presente documento. Así mismo, el Usuario asume cualquier consecuencia derivada del uso no apropiado de dichas facilidades, sea esta administrativa, laboral, civil o penal.

3. Son expresamente prohibidas las siguientes acciones:

   - Envío de correo electrónico de carácter personal que resulte masivo y/o no solicitado.

   - Propagación de cadenas de mensajes.

   - Publicación de anuncios personales sin autorización de la Organización (servicios, productos, objetos y otros).

- No se permite bajo ninguna circunstancia el uso de de las computadoras con propósito de ocio o lucro.

DATOS

Amenaza: [E.2] Errores del administrador.

1. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

2. El Administrador de sistemas se encargará de evaluar el incidente ó el error, trazar un plan de acción, llevarlo a cabo, comprobar los resultados y actuar en consecuencia.

3. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [E.1] Errores de los usuarios.

1. Debe existir capacitación u orientación a los usuarios que utilizan cada uno de los servicios pertenecientes a la institución.

2. El Administrador de sistemas se encargará de evaluar el incidente ó el error, trazar un plan de acción, llevarlo a cabo, comprobar los resultados y actuar en consecuencia.

3. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

4. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos

Amenaza: [E.17] Degradación de la información.

1. Se debe hacer copias de seguridad en diferentes medios de almacenamiento diferentes para cada uno de los datos.

2. La información de la compañía clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando software de encriptado robusto. El acceso a las claves utilizadas para el cifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

3. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

4. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [E.19] Divulgación de información.

1. No pueden extraerse datos fuera de la sede de la Compañía sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.

2. La información confidencial en lo posible no debe dejarse al alcance de personal no autorizado.

Amenaza: [A.15] Modificación de información [A.16] Introducción de falsa información

1. El usuario que dispone de la información debe estar previamente autorizado por el administrador del sistema. Es decir que el usuario debe gozar de los privilegios suficientes para acceder a dicha información.

2. Los datos de entrada y salida del sistema deberán poseer controles donde se verifique su integridad, exactitud y validez.

3. No se pueden extraer los datos fuera de la compañía.

4. La información de la compañía clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando software de encriptado robusto. El acceso a las claves utilizadas para el cifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

5. No se debe realizar ningún tipo de operación sobre la información por personal que no este autorizado.

6. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

7. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

Amenaza: [E.15] Alteración de la información [E.16] Introducción de falsa información [E.17] Degradación de la información.

A.12.2.2

1. No se debe realizar ningún tipo de operación sobre la información por personal que no este autorizado.

2. Se debe hacer copias de seguridad en diferentes medios de almacenamiento diferentes para cada uno de los datos.

3. La información confidencial en lo posible no debe dejarse al alcance de personal no autorizado.

4. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

5. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

6. La información de la compañía clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando software de encriptado robusto. El acceso a las claves utilizadas para el cifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

Amenaza: [A.11] Acceso no autorizado

1. Se establecerán las medidas y normas oportunas para restringir los accesos a las zonas previamente establecidas, de forma que sólo se pueda acceder a los recursos asignados aquellos que sean autorizados y tengan esos privilegios.

2. Debe existir procedimientos o sistemas de control automatizados que le permitan al administrador conocer en cualquier momento los accesos al sistema por usuarios autorizados o no.

3. Debe existir sistema de control que permitan al administrador de la planta o espacio físico conocer el acceso a las áreas críticas por personal no autorizado.

4. El acceso del personal autorizado de procesamiento así como el personal contratado sólo podrá permanecer en las instalaciones de las empresas durante el horario autorizado.

5. Los empleados que actualmente no se encuentran vinculados con la institución se les aplicara un procedimiento de baja de todas las cuentas de usuarios y privilegios de acceso.

6. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

7. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

8. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

Amenaza: [E.18] Destrucción de la información

1. Se debe hacer copias de seguridad en diferentes medios de almacenamiento diferentes para cada uno de los datos.

2. La información confidencial en lo posible no debe dejarse al alcance de personal no autorizado.

3. Toda información que deje de ser útil a la institución deberá ser borrada únicamente con previa autorización y supervisión de los administradores del sistema y responsable de dichos datos, esto se realizara bajo procedimientos detallados.

4. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

5. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

6. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos

SOPORTES DE INFORMACION

Amenaza: [I.10] Degradación de los soportes de almacenamiento de la información.

1. Se debe hacer copias de seguridad en diferentes medios de almacenamiento diferentes para cada uno de los datos.

2. El administrador del sistema será el encargado de realizar respaldos periódicamente cada mes.

3. Se debe realizar mantenimiento y verificación de las condiciones de cada uno de los soportes de información.

4. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

Amenaza: [N.1] Fuego [N.2] Daños por agua [I.1] Fuego

1. Deberá generarse una documentación, con información correcta, consistente y actualizada, sobre normas y procedimientos de seguridad industrial. Deberá asignarse un responsable a cargo de la gestión de la documentación y de la seguridad industrial en la empresa.

2. Deberán existir procedimientos detallados a seguir por el personal en caso de emergencias, indicando responsables, quiénes deben estar adecuadamente capacitados.

3. Las instalaciones y todos sus activos deberán contar mecanismos de prevención y control de desastres.

Amenaza: [A.25] Robo

1. Debe existir sistema de control que permitan al administrador de la planta o espacio físico conocer el acceso a as áreas críticas por personal no autorizado.

2. Realizar un control de entrada y salida del establecimiento.

3. Deberá generarse una documentación, con información correcta, consistente y actualizada, sobre normas y procedimientos de seguridad industrial. Deberá asignarse un responsable a cargo de la gestión de la documentación y de la seguridad industrial en la empresa.

Amenaza: [I.5] Avería de origen físico o lógico.

1. Cualquier falla en los computadores o en la red debe reportarse inmediatamente al administrador de sistema ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

2. Se deben realizar periódicamente procedimientos concernientes al mantenimiento de hardware y software a cada unos de los equipos del Tic Solution.

3. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

4. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos

EQUIPAMIENTO AUXILIAR

Amenaza: [I.6] Corte del suministro eléctrico

1. Periódicamente lo generadores eléctricos y los sistemas de alimentación interrumpida como las UPS presentes en el Tic Solution deben ser sometidos a mantenimiento y revisión periódica.

2. Se deben usar estabilizadores de energía eléctrica en los PCS y demás equipos y en los servidores y estaciones críticas deben usarse fuentes de poder ininterrumpibles (UPS).

3. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

4. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [N.*] Desastres naturales [N.1] Fuego [N.2] Daños por agua [I.*] Desastres industriales [I.1] Fuego [I.2] Daños por agua.

1. Deberá generarse una documentación, con información correcta, consistente y actualizada, sobre normas y procedimientos de seguridad industrial. Deberá asignarse un responsable a cargo de la gestión de la documentación y de la seguridad industrial en la empresa.

2. Deberán existir procedimientos detallados a seguir por el personal en caso de emergencias, indicando responsables, quiénes deben estar adecuadamente capacitados.

3. Las instalaciones y todos sus activos deberán contar mecanismos de prevención y control de desastres.

Amenaza: [I.5] Avería de origen físico o lógico

1. Cualquier falla en el equipamiento auxiliar debe reportarse inmediatamente al jefe de seguridad ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

2. Se deben realizar periódicamente procedimientos concernientes al mantenimiento del equipamiento auxiliar del Tic Solution.

3. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

4. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos

Amenaza: [I.7] Condiciones inadecuadas de temperatura y/o Humedad

1. Los equipos deben encontrase en un ambiente adecuado y seguro donde se encuentren alejados del fuego, humo, polvo y temperaturas extremas.

Amenaza: [A.25] Robo

4. Debe existir sistema de control que permitan al administrador de la planta o espacio físico conocer el acceso a as áreas críticas por personal no autorizado.

5. Realizar un control de entrada y salida del establecimiento.

6. Deberá generarse una documentación, con información correcta, consistente y actualizada, sobre normas y procedimientos de seguridad industrial. Deberá asignarse un responsable a cargo de la gestión de la documentación y de la seguridad industrial en la empresa.

EQUIPOS DE COMUNICACIONES

Amenaza: [I.5] Avería de origen físico o lógico

1. Cualquier falla en los computadores o en la red debe reportarse inmediatamente al jefe de seguridad ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

2. Se deben usar estabilizadores de energía eléctrica en los PCs y para los Servidores deben usarse fuentes de poder ininterrumpibles (UPS).

3. Se debe realizar mantenimiento a hardware y software programados cada mes.

Amenaza: [I.6] Corte del suministro eléctrico.

1. Periódicamente lo generadores eléctricos y los sistemas de alimentación interrumpida como las UPS presentes en el Tic Solution deben ser sometidos a mantenimiento y revisión periódica.

2. Se deben usar estabilizadores de energía eléctrica en los PCS y demás equipos y en los servidores y estaciones críticas deben usarse fuentes de poder ininterrumpibles (UPS).

3. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

4. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos

Amenaza: [I.7] Condiciones inadecuadas de temperatura y/o humedad.

1. Los equipos deben encontrase en un ambiente adecuado y seguro donde se encuentren alejados del fuego, humo, polvo y temperaturas extremas.

Amenaza: [A.24] Denegación de servicio

1. Los equipos de red deben estar aislados de acceso de personal inapropiado.

2. Las redes de datos tienen que estar aisladas del cableado eléctrico.

3. Cualquier incorporación de cualquier equipo nuevo en la red se deberá realizar con previo permiso y autorización del sistema administrador.

4. Los dispositivos de nertworking, equipos de cómputo y la red del centro de Tic Solution deben contar y cumplir con especificaciones y estándares necesarios para brindar una buena calidad de servicio.

5. Esta estrictamente prohibido utilizar herramientas propias de delincuentes informáticos, tales como programas que rastrean vulnerabilidades en sistemas de computo propios u ajenos.

6. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

7. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos

Amenaza: [N.*] Desastres naturales [I.1] Fuego [I.*] Desastres industriales [I.2] Daños por agua

1. Deberá generarse una documentación, con información correcta, consistente y actualizada, sobre normas y procedimientos de seguridad industrial. Deberá asignarse un responsable a cargo de la gestión de la documentación y de la seguridad industrial en la empresa.

2. Deberán existir procedimientos detallados a seguir por el personal en caso de emergencias, indicando responsables, quiénes deben estar adecuadamente capacitados.

3. Las instalaciones y todos sus activos deberán contar mecanismos de prevención y control de desastres.

Amenaza: [E.2] Errores del administrador

1. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la Empresa.

2. El Administrador de seguridad se encargará de evaluar el incidente ó el error, trazar un plan de acción, llevarlo a cabo, comprobar los resultados y actuar en consecuencia.

3. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [A.25] Robo

1. Debe existir sistema de control que permitan al administrador de la planta o espacio físico conocer el acceso a as áreas críticas por personal no autorizado.

2. Realizar un control de entrada y salida del establecimiento.

3. Los gabinetes donde se ubican los switches de cada una de las oficinas, deberán permanecer guardados bajo llave, y fuera del alcance de personal no autorizado.

Amenaza: [E.4] Errores de configuración

1. Deben existir sistemas de control automatizados que le permitan al administrador conocer en cualquier momento los accesos al sistema por usuarios autorizados o no autorizados, así como también conocer las actividades realizadas durante los

accesos a los programas. Además se debe controlar la instalación o desinstalación de programas licenciados o no.

2. Las configuraciones de cada uno de los dispositivos de interconexión de red, equipos de cómputo y aplicaciones deben ser almacenadas en manuales y en copias de seguridad.

3. Debe implantarse un sistema de autorización y control de acceso a los equipos de cómputos y redes, con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos o configuraciones importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

4. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

5. Deberán existir estándares de configuración de los puestos de trabajo, servidores y demás equipos de la red de la información. Con base al estándar se deberá generar un procedimiento donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.

6. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción.

7. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

EQUIPAMIENTO INFORMATICO

Amenaza: [I.5] Avería de origen físico o lógico

1. Cualquier falla en los computadores o en la red debe reportarse inmediatamente al administrador ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

2. Se deben usar estabilizadores de energía eléctrica en los PCs y para los Servidores deben usarse fuentes de poder ininterrumpibles (UPS).

3. Los equipos deben mantenerse aseados

4. Se debe realizar mantenimiento a hardware y software programados cada mes.

Amenaza: [I.6] Corte del suministro eléctrico

1. Se deben usar estabilizadores de energía eléctrica en los PCS y para los Servidores y equipos críticos deben usarse fuentes de poder ininterrumpibles (UPS).

Amenaza: [I.7] Condiciones inadecuadas de temperatura y/o humedad.

1. Los equipos deben encontrase en un ambiente adecuado alejados del fuego, humo, polvo y temperaturas extremas.

2. Mantener los equipos fuera del alcance de rayos, agua, vibraciones.

Amenaza: [A.24] Denegación de servicio.

1. Los equipos de red deben estar aislados de acceso de personal inapropiado.

2. Las redes de datos tienen que estar aisladas del cableado eléctrico.

3. Se deberá pedir permiso al administrador para conectar un equipo nuevo a la red.

4. Los dispositivos de nertworking, equipos de cómputo y la red del centro de Tic Solution (servidores y estaciones de trabajo) deben contar y cumplir con especificaciones y estándares necesarios para brindar una buena calidad de servicio.

5. Esta estrictamente prohibido utilizar herramientas propias de delincuentes informáticos, tales como programas que rastrean vulnerabilidades en sistemas de computo propios u ajenos.

6. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

7. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [A.25] Robo

1. Debe existir sistema de control que permitan al administrador de la planta o espacio físico conocer el acceso a as áreas críticas por personal no autorizado.

2. Realizar un control de entrada y salida del establecimiento.

3. Los gabinetes donde se ubican los switches de cada una de las oficinas, deberán permanecer guardados bajo llave, y fuera del alcance de personal no autorizado.

4. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [N.*] Desastres naturales [N.2] Daños por agua [N.1] Fuego [I.2] Daños por agua

1. Deberá generarse una documentación, con información correcta, consistente y actualizada, sobre normas y procedimientos de seguridad industrial. Deberá asignarse un responsable a cargo de la gestión de la documentación y de la seguridad industrial en la empresa.

2. Deberán existir procedimientos detallados a seguir por el personal en caso de emergencias, indicando responsables, quiénes deben estar adecuadamente capacitados.

3. Deberá existir una llave de corte de energía general en la salida de emergencias del edificio.

4. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

Amenaza: [A.4] Manipulación de la configuración

1. Debe implantarse un sistema de autorización y control de acceso a los equipos de cómputos y redes, con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos o configuraciones importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

2. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la empresa.

3. Deberán existir estándares de configuración de los puestos de trabajo, servidores y demás equipos de la red de la información. Con base al estándar se deberá generar un procedimiento donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.

4. La empresa sancionara disciplinariamente a aquella persona que haya cometido un incidente de seguridad o no haya acatado las políticas de seguridad; esta será sometida a evaluación para valorar el incidente y posteriormente imponer una sanción

5. Las configuraciones de cada uno de los dispositivos de interconexión de red, equipos de cómputo y aplicaciones deben ser almacenadas en manuales y en copias de seguridad.

6. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos

Amenaza: [E.2] Errores del administrador

1. Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en la Empresa.

2. El Administrador de seguridad se encargará de evaluar el incidente ó el error, trazar un plan de acción, llevarlo a cabo, comprobar los resultados y actuar en consecuencia.

3. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

PERSONAL

Amenaza: [A.28] Indisponibilidad del personal. **Amenaza:** [E.28] Indisponibilidad del personal.

1. El personal debe cumplir con las funciones y responsabilidades laborales acogiéndose a los reglamentos y políticas establecidas en el Tic Solution:

INSTALACIONES

Amenaza: [N.*] Desastres naturales [N.2] Daños por agua [N.1] Fuego [I.2] Daños por agua

1. Deberá generarse una documentación, con información correcta, consistente y actualizada, sobre normas y procedimientos de seguridad industrial. Deberá asignarse un responsable a cargo de la gestión de la documentación y de la seguridad industrial en la empresa.

2. Deberán existir procedimientos detallados a seguir por el personal en caso de emergencias, indicando responsables, quiénes deben estar adecuadamente capacitados.

3. Deberá existir una llave de corte de energía general en la salida de emergencias del edificio.

4. Se deberán documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar la severidad del incidente, y las acciones a tomar que sean necesarias para la protección y control de los datos.

CONTROLES

A continuación se enuncian los controles a aplicar en cada una de las políticas de seguridad diseñadas para el Tic Solution TIC SOLUTION. Los controles se tomaron de la **ISO/IEC 27002:2005**

ACTIVO	AMENAZA	CONTROL
Aplicaciones		
	[E.8] [A.8]	**(1)**[A.10.4.1] **(2)**[A.10.10.2] - [A.12.4.1] **(3)** [A.12.4.1] - [A.10.4.2] - [A.11.4.4] **(4)** [A.8.2.2] **(6,7)** [A.10.1.1] **(5)**[A.8.2.3]
	[A.4] [E.4]	**(1)** [A.10.10.1] - [A.10.10.2] **(2)**[A.10.10.4] **(3)** [A.11.2.2] - [A.11.4.1] - [A.11.5.2] - [A.11.6.1] **(4,7)**[A.10.1.1] **(5)**[A.14.1.4] - [A.11.2.2] **(6)**[A.8.2.3]
	[E.21]	**(1)**[A.9.2.4]-[A.10.3.2]-[A.12.5] **(2,3)**[A.10.1.1]
	[E.20]	**(1)**[A.12.2] - [A.12.5] **(2)**[A.12.6.1] - [A.10.4] -[A.12.2.1] **(3)**[A.10.4.2]- [A.11.4.4] - [A.12.4.1] **(4)**[A.8.2.3] **(5 Y 6)**[A.10.1.1]
	[A.5]	**(1)**[A.11.5.2] - [A.11.5.3] **(2,3)**[A.11.2] **(4,5)**[A.11.3.1] -[A.12.2.1] -[A.11.3.2] **(6)** [A.8.2.3]

		(7)[A.8.3.3] **(8 y 9)** [A.10.1.1] – [A.10.1.2]
	[A.11]	**(1,3)** [A.9.1.2] - [A.9.1.5] - [A.9.1.1] - [A.10.1.4] -[A.11.2.1] [A.11.4.1] - [A.11.6.1] - [A.12.4.3] - [A.12.2.1] **(2)** [A10.10.1] - [A.10.10.4] - [A.10.10.6] **(5)** [A.8.3] **(8)** [A.13.2.3] - [A.15.1] **(6,7)** [A.10.1.1]
Servicios		
	[A.24]	**(1,3)** [A.10.3] - [A.9.2.2] - [A.14.1.2] - [A.14.1.3] - [A.10.1.1] **(4)** [A.13.2] **(5)**[A.10.10.5] **(6,7)**[A.10.1.1] **(9)** [A.8.2.3] **(10) (3)**[A.10.4.2]- [A.11.4.4] - [A.12.4.1]
	[E.1]	**(1)**[A.8.2] **(2,3)**[A.10.10.5] - [A.10.1.1]
	[A.4] [E.4]	**(1)** [A.10.10.1] - [A.10.10.2] **(2)**[A.10.10.4] **(3)** [A.11.2.2] - [A.11.4.1] - [A.11.5.2] - [A.11.6.1] **(4,7)**[A.10.1.1] **(5)**[A.14.1.4] - [A.11.2.2] **(6)**[A.8.2.3]

	[A.5]	**(1)**[A.11.5.2] - [A.11.5.3] **(2,3)**[A.11.2] **(4,5)**[A.11.3.1] -[A.12.2.1] -[A.11.3.2] **(6)** [A.8.2.3] **(7)**[A.8.3.3] **(8 y 9)** [A.10.1.1] – [A.10.1.2]
	[E.2]	**(1)[**A.10.1.1] **(2)[**A.13.2]-[A.14.1] **(3)** [A.10.1.1] - [A.13.2]
	[A.7]	**(1,2,3)**[A.8.2.2]- [A.15.1.5]
Datos		
	[E.2]	**(1)[**A.10.1.1] **(2)[**A.13.2] - [A.14.1] **(3)** [A.10.1.1] - [A.13.2] A. 5.1.1 - 5.1.2
	[E.1]	**(1)**[A.8.2] **(2)**[A.10.10.5] **(3)** [A.10.1.1]
	[E.17]	**(1)**[A.10.5.1] **(2)**[A.12.3] **(3,4)**[A.10.1.1]
	[E.19]	**(1)**[A.15.1.4] **(2)**[A.6.1.5]
	[A.15] [A.16]	**(1)[**A.11.6.1] **(2)**[A.12.2.1] **(5y6)**[A.10.1.1] **(3)[**A.6.1.5] **(4)**[A.12.3]
	[E.15] [E.16] [E.17]	**(1)[**A.11.6.1] - [A.10.7.4] - [A.10.8.3] -[A.10.10.3] - [A.11.4.1] **(2)**[A.10.5.1] **(3)**[A.6.1.5]

		(6)[A.12.3] **(4,5)** [A.10.1.1]
	[A.11]	**(1,3)** [A.9.1.2] - [A.9.1.5] - [A.9.1.1] - [A.10.1.4] -[A.11.2.1] [A.11.4.1] - [A.11.6.1] - [A.12.4.3] - [A.12.2.1] **(2)** [A10.10.1] - [A.10.10.4] - [A.10.10.6] **(5)** [A.8.3] **(8)** [A.13.2.3] - [A.15.1] **(6,7)** [A.10.1.1]
	[E.18]	**(1)** [A.12.2.1] **(2)[**A.6.1.5] **(5,6)**[A.10.1.1] **(3)[**A.10.7.2] **(4)** [A.13.2.3]
Soportes de Información		
	[I.10]	**(1)** [A.12.2.1] **(2)[**A.6.1.5] **(4)**[A.10.1.1] **(3)[**A.9.2.4]
	[N.1] [N.2] [I.1]	**(1)** [A.10.1.1] **(2)**[A.15.2.1] **(3)**[A.14.1] - [A.9.1.4]
	[A.25]	**(1,2)** [A.9.1.1] - [A.9.1.2] - [A.9.1.3] - [A.9.1.5] -[A.9.1.6] **(3)**[A.10.1.1]
	[I.5]	**(1)**[A.10.10.5] **(2)**[A.9.2.4] **(3 y 4)**[A.10.1.1]

Equipamiento Auxiliar	**[I.6]**	**(1y 2)**[A.9.2.2] **(3 y 4)**[A.10.1.1]
	[I.2] [N.1] [N.2] [I.*] [I.1] [N.*]	**(1)** [A.10.1.1] **(2)**[A.15.2.1] **(3)**[A.14.1] - [A.9.1.4]
	[I.5]	**(1)**[A.10.10.5] **(2)**[A.9.2.4] **(3 y 4)**[A.10.1.1]
	[I.7]	**(1)**[A.9.2.1]
	[A.25]	**(1,2)** [A.9.1.1] - [A.9.1.2] - [A.9.1.3] - [A.9.1.5] - [A.9.1.6] **(3)**[A.10.1.1]
Equipos de Comunicaciones		
	[I.5]	**(1)**[A.10.10.5] **(2)**[A.9.2.4] **(3 y 4)**[A.10.1.1]
	[I.6]	**(1y 2)**[A.9.2.2] **(3 y 4)**[A.10.1.1]
	[I.7]	**(1)**[A.9.2.1]
	[A.24]	**(1,3)**[A.10.3] - [A.9.2.2] - [A.14.1.2] - [A.14.1.3] - [A.10.1.1] **(4)** [A.13.2] **(5)[**A.10.10.5] **(6,7)**[A.10.1.1]
	[I.2] [N.1] [N.2] [I.*] [I.1] [N.*]	**(1)** [A.10.1.1] **(2)**[A.15.2.1] **(3)**[A.14.1] - [A.9.1.4]
	[E.2]	**(1)[**A.10.1.1] **(2)[**A.13.2] - [A.14.1] **(3)[**A.10.1.1] - [A.13.2]
	[A.25]	**(1,2)** [A.9.1.1] - [A.9.1.2] - [A.9.1.3] - [A.9.1.5] - [A.9.1.6] **(3)**[A.10.1.1]
	[E.4]	**(1)**[A.10.10.1] - [A.10.10.2]

		(3)[A.11.2.2] - [A.11.4.1] - [A.11.5.2] - [A.11.6.1] - [A.10.10.4] **(4,7)**[A.10.1.1] **(5)** [A.14.1.4] [A.11.2.2]
Equipamiento Informático		
	[I.5]	**(1)**[A.10.10.5] **(2)**[A.9.2.4] **(3 y 4)**[A.10.1.1]
	[I.6]	**(1y 2)**[A.9.2.2] **(3 y 4)**[A.10.1.1]
	[I.7]	**(1)**[A.9.2.1]
	[A.24]	**1,3)**[A.10.3] - [A.9.2.2] - [A.14.1.2] - [A.14.1.3] - [A.10.1.1] **(4)** [A.13.2] **(5)[**A.10.10.5] **(6,7)**[A.10.1.1]
		(5)[A.10.10.5] **(6,7)[**A.10.1.1]
	[A.25]	**(1,2)** [A.9.1.1] - [A.9.1.2] - [A.9.1.3] - [A.9.1.5] - [A.9.1.6] **(3)**[A.10.1.1]
	[I.2] [N.1] [N.2] [I.*] [I.1] [N.*]	**(1)** [A.10.1.1] **(2)**[A.15.2.1] **(3)**[A.14.1] - [A.9.1.4]
	[A.4]	**(1)[**A.10.10.1] - [A.10.10.2]
		(3)[A.11.2.2] - [A.11.4.1] - [A.11.5.2] - [A.11.6.1] - [A.10.10.4] **(4,7)[**A.10.1.1] **(5)** A.14.1.4 A.11.2.2
	[E.2]	**(1)[**A.10.1.1] **(2)[**A.13.2] - [A.14.1] **(3)** [A.10.1.1] - [A.13.2]
Personal		

	[A.28] [E.28]	**(1)[**A.8.1.1]
Instalaciones		
	[I.2] [N.1] [N.2] [I.*] [I.1] [N.*]	**(1)** [A.10.1.1] **(2)**[A.15.2.1] **(4)**[A.14.1] - [A.9.1.4]

RIESGO RESIDUAL

El riesgo residual que se detallara a continuación es tomado como referencia de la escala enumerada en los criterios de valoración planteados en el apartado 4 (Criterios de Valoración) del libro Catalogo de Elementos de la metodología Magerit V2, donde se define que después de realizar la implementación de salvaguardas la disminución del riesgo en el activo afectado es de un 70% en promedio, cabe resaltar que este valor es suministrado de manera estimativa.

ACTIVOS/AMENAZAS	Riesgo	Tipo riego	RIESGO RESIDUAL	
[SW_Fin2000] Finanzas2000			Riesgo Residual	Tipo de riesgo Residual
[E.1] Errores de los usuarios	1	Trivial	0,7	Trivial
[E.4] Errores de configuración	4	Trivial	2,8	Trivial
[E.8] Difusión de software dañino	15	Importante	10,5	Moderado
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.8] Difusión de software dañino	5	Tolerable	3,5	Trivial

[E.21] Errores de mantenimiento / actualización	4	Trivial	2,8	Trivial
[E.20] Vulnerabilidades de los programas (software)	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas (software)	5	Tolerable	3,5	Trivial
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[E.4] Errores de configuración	2	Trivial	1,4	Trivial
[E.20] Vulnerabilidades de los programas (software)	2	Trivial	1,4	Trivial
[A.4] Manipulación de la configuración	2	Trivial	1,4	Trivial
[A.5] Suplantación de la identidad del usuario	3	Trivial	2,1	Trivial
[A.5] Suplantación de la identidad del usuario	6	Tolerable	4,2	Tolerable
[E.4] Errores de configuración	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[A.11] Acceso no autorizado	6	Tolerable	4,2	Tolerable
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial

[SW_Spem] Servicio público de empleo	Riesgo	Tipo riego	Riesgo Residual	Tipo de riesgo Residual
[E.1] Errores de los usuarios	2	Trivial	1,4	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[E.8] Difusión de software dañino	18	Importante	12,6	Moderado
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[A.8] Difusión de software dañino	6	Tolerable	4,2	Tolerable
[E.20] Vulnerabilidades de los programas(software)	6	Tolerable	4,2	Tolerable
[E.21] Errores de mantenimiento / actualización	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial

[A.5] Suplantación de la identidad del usuario	8	Tolerable	5,6	Tolerable
[E.4] Errores de configuración	4	Tolerable	2,8	Trivial
[A.4] Manipulación de la configuración	4	Tolerable	2,8	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[A.11] Acceso no autorizado	4	Trivial	2,8	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[SW_web_regi] Pagina web de la regional Bolívar	**Riesgo**	**Tipo riego**	**Riesgo Residual**	**Tipo de riesgo Residual**
[E.1] Errores de los usuarios	2	Trivial	1,4	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[E.8] Difusión de software dañino	18	Importante	12,6	Moderado
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[A.8] Difusión de software dañino	6	Tolerable	4,2	Tolerable
[E.20] Vulnerabilidades de los programas(software)	6	Tolerable	4,2	Tolerable
[E.21] Errores de mantenimiento / actualización	5	Tolerable	3,5	Trivial

[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[E.4] Errores de configuración	4	Tolerable	2,8	Trivial
[A.4] Manipulación de la configuración	4	Tolerable	2,8	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[A.11] Acceso no autorizado	4	Trivial	2,8	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[SW_SAGC] sistema académico de gestión de centro	**Riesgo**	**Tipo riego**	**Riesgo Residual**	**Tipo de riesgo Residual**
[E.1] Errores de los usuarios	2	Trivial	1,4	Trivial
[E.4] Errores de configuración	6	Tolerable	4,2	Tolerable
[E.8] Difusión de software dañino	21	Intolerable	14,7	Moderado
[A.4] Manipulación de la configuración	7	Tolerable	4,9	Tolerable
[A.8] Difusión de software dañino	7	Tolerable	4,9	Tolerable

[E.20] Vulnerabilidades de los programas(software)	7	Tolerable	4,9	Tolerable
[E.21] Errores de mantenimiento / actualización	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas (software)	7	Tolerable	4,9	Tolerable
[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	8	Tolerable	5,6	Tolerable
[E.4] Errores de configuración	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[A.5] Suplantación de la identidad del usuario	6	Tolerable	4,2	Tolerable
[A.11] Acceso no autorizado	6	Tolerable	4,2	Tolerable

[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[SW_SGVA] sistema de gestión virtual de aprendices	**Riesgo**	**Tipo riego**	Riesgo Residual	Tipo de riesgo Residual
[E.1] Errores de los usuarios	2	Trivial	1,4	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[E.8] Difusión de software dañino	18	Importante	12,6	Moderado
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[A.8] Difusión de software dañino	6	Tolerable	4,2	Tolerable
[E.20] Vulnerabilidades de los programas(software)	6	Tolerable	4,2	Tolerable
[E.21] Errores de mantenimiento / actualización	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[E.20] Vulnerabilidades de los programas (software)	4	Trivial	2,8	Trivial
[A.4] Manipulación de la configuración	4	Trivial	2,8	Trivial
[E.4] Errores de configuración	2	Trivial	1,4	Trivial

[E.20] Vulnerabilidades de los programas (software)	3	Trivial	2,1	Trivial
[A.4] Manipulación de la configuración	2	Trivial	1,4	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
			0	
[E.4] Errores de configuración	3	Tolerable	2,1	Trivial
[A.4] Manipulación de la configuración	3	Tolerable	2,1	Trivial
[A.5] Suplantación de la identidad del usuario	3	Trivial	2,1	Trivial
[A.11] Acceso no autorizado	3	Trivial	2,1	Trivial
[A.5] Suplantación de la identidad del usuario	2	Trivial	1,4	Trivial
[SW_Adm2000] Administración 2000	**Riesgo**	**Tipo riego**	**Riesgo Residual**	**Tipo de riesgo Residual**
[E.1] Errores de los usuarios	1	Trivial	0,7	Trivial
[E.4] Errores de configuración	4	Trivial	2,8	Trivial
[E.8] Difusión de software dañino	15	Importante	10,5	Moderado
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.8] Difusión de software dañino	5	Tolerable	3,5	Trivial

[E.20] Vulnerabilidades de los programas(software)	5	Tolerable	3,5	Trivial
[E.21] Errores de mantenimiento / actualización	4	Trivial	2,8	Trivial
[E.20] Vulnerabilidades de los programas (software)	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas (software)	5	Tolerable	3,5	Trivial
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[E.4] Errores de configuración	2	Trivial	1,4	Trivial
[E.20] Vulnerabilidades de los programas (software)	2	Trivial	1,4	Trivial
[A.4] Manipulación de la configuración	2	Trivial	1,4	Trivial
[A.5] Suplantación de la identidad del usuario	3	Trivial	2,1	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[A.11] Acceso no autorizado	5	Tolerable	3,5	Trivial

[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[SW_Cactus] Biodata	**Riesgo**	**Tipo riego**	Riesgo Residual	Tipo de riesgo Residual
[E.1] Errores de los usuarios	1	Trivial	0,7	Trivial
[E.4] Errores de configuración	4	Trivial	2,8	Trivial
[E.8] Difusión de software dañino	15	Importante	10,5	Moderado
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.8] Difusión de software dañino	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas(software)	5		3,5	Trivial
[E.21] Errores de mantenimiento / actualización	4	Trivial	2,8	Trivial
[E.20] Vulnerabilidades de los programas (software)	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas (software)	4	Trivial	2,8	Trivial
[A.4] Manipulación de la configuración	4	Trivial	2,8	Trivial
[E.4] Errores de configuración	3	Trivial	2,1	Trivial
[E.20] Vulnerabilidades de los programas (software)	4	Trivial	2,8	Trivial

[A.4] Manipulación de la configuración	3	Trivial	2,1	Trivial
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.11] Acceso no autorizado	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[SW_Tarant]tarantela nomina	**Riesgo**	**Tipo riego**	Riesgo Residual	Tipo de riesgo Residual
[E.1] Errores de los usuarios	2	Trivial	1,4	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[E.8] Difusión de software dañino	18	Importante	12,6	Moderado
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[A.8] Difusión de software dañino	6	Tolerable	4,2	Tolerable
[E.20] Vulnerabilidades de los programas(software)	6	Tolerable	4,2	Tolerable
[E.21] Errores de mantenimiento / actualización	5	Tolerable	3,5	Trivial

[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[E.4] Errores de configuración	3	Trivial	2,1	Trivial
[E.20] Vulnerabilidades de los programas (software)	4	Trivial	2,8	Trivial
[A.4] Manipulación de la configuración	3	Trivial	2,1	Trivial
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	6	Tolerable	4,2	Tolerable
[E.4] Errores de configuración	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[A.11] Acceso no autorizado	6	Tolerable	4,2	Tolerable
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[SW_Aport] Aportes	**Riesgo**	**Tipo riego**	Riesgo Residual	Tipo de riesgo Residual
[E.1] Errores de los usuarios	2	Trivial	1,4	Trivial

[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[E.8] Difusión de software dañino	18	Importante	12,6	Moderado
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[A.8] Difusión de software dañino	6	Tolerable	4,2	Tolerable
[E.20] Vulnerabilidades de los programas(software)	6	Tolerable	4,2	Tolerable
[E.21] Errores de mantenimiento / actualización	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[E.4] Errores de configuración	4	Trivial	2,8	Trivial
[E.20] Vulnerabilidades de los programas (software)	5	Tolerable	3,5	Trivial
[A.4] Manipulación de la configuración	4	Trivial	2,8	Trivial
[A.5] Suplantación de la identidad del usuario	6	Tolerable	4,2	Tolerable

[A.5] Suplantación de la identidad del usuario	6	Tolerable	4,2	Tolerable
[E.4] Errores de configuración	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[A.11] Acceso no autorizado	6	Tolerable	4,2	Tolerable
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[SW_os]sistemas operativos	**Riesgo**	**Tipo riego**	Riesgo Residual	Tipo de riesgo Residual
[E.1] Errores de los usuarios	1	Trivial	0,7	Trivial
[E.4] Errores de configuración	4	Trivial	2,8	Trivial
[E.8] Difusión de software dañino	15	Importante	10,5	Moderado
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.8] Difusión de software dañino	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas(software)	5	Tolerable	3,5	Trivial
[E.21] Errores de mantenimiento / actualización	4	Trivial	2,8	Trivial
[E.20] Vulnerabilidades de los programas (software)	5	Tolerable	3,5	Trivial

[E.20] Vulnerabilidades de los programas (software)	5	Tolerable	3,5	Trivial
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[E.4] Errores de configuración	4	Trivial	2,8	Trivial
[E.20] Vulnerabilidades de los programas (software)	5	Tolerable	3,5	Trivial
[A.4] Manipulación de la configuración	4	Tolerable	2,8	Trivial
[A.5] Suplantación de la identidad del usuario	6	Tolerable	4,2	Tolerable
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[E.4] Errores de configuración	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[SW_av]antivirus	**Riesgo**	**Tipo riego**	**Riesgo Residual**	**Tipo de riesgo Residual**
[E.1] Errores de los usuarios	0	Trivial	0	Trivial
[E.4] Errores de configuración	2	Trivial	1,4	Trivial
[E.8] Difusión de software dañino	6	Tolerable	4,2	Tolerable

[A.4] Manipulación de la configuración	2	Trivial	1,4	Trivial
[A.8] Difusión de software dañino	2	Trivial	1,4	Trivial
[E.20] Vulnerabilidades de los programas(software)	2	Trivial	1,4	Trivial
[E.21] Errores de mantenimiento / actualización	2	Trivial	1,4	Trivial
[E.20] Vulnerabilidades de los programas (software)	2	Trivial	1,4	Trivial
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.11] Acceso no autorizado	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[SW_Edpro] Editores para el diseño y programación	**Riesgo**	**Tipo riego**	**Riesgo Residual**	**Tipo de riesgo Residual**
[E.1] Errores de los usuarios	0	Trivial	0	Trivial
[E.4] Errores de configuración	2	Trivial	1,4	Trivial
[E.8] Difusión de software dañino	6	Tolerable	4,2	Tolerable

[A.4] Manipulación de la configuración	2	Trivial	1,4	Trivial
[A.8] Difusión de software dañino	2	Trivial	1,4	Trivial
[E.20] Vulnerabilidades de los programas(software)	2	Trivial	1,4	Trivial
[E.21] Errores de mantenimiento / actualización	2	Trivial	1,4	Trivial
[E.20] Vulnerabilidades de los programas (software)	2	Trivial	1,4	Trivial
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.11] Acceso no autorizado	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[SW_dbms] sistemas de gestión de bases de datos	**Riesgo**	**Tipo riego**	**Riesgo Residual**	**Tipo de riesgo Residual**
[E.1] Errores de los usuarios	2	Trivial	1,4	Trivial
[E.4] Errores de configuración	6	Tolerable	4,2	Tolerable
[E.8] Difusión de software dañino	21	Intolerable	14,7	Moderado

[A.4] Manipulación de la configuración	7	Tolerable	4,9	Tolerable
[A.8] Difusión de software dañino	7	Tolerable	4,9	Tolerable
[E.20] Vulnerabilidades de los programas(software)	7	Tolerable	4,9	Tolerable
[E.21] Errores de mantenimiento / actualización	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas (software)	7	Tolerable	4,9	Tolerable
[E.20] Vulnerabilidades de los programas (software)	7	Tolerable	4,9	Tolerable
[A.4] Manipulación de la configuración	7	Tolerable	4,9	Tolerable
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas (software)	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	8	Tolerable	5,6	Tolerable
[A.5] Suplantación de la identidad del usuario	6	Tolerable	4,2	Tolerable
[E.4] Errores de configuración	6	Tolerable	4,2	Tolerable

[A.4] Manipulación de la configuración	6	Tolerable	4,2	Tolerable
[A.11] Acceso no autorizado	6	Tolerable	4,2	Tolerable
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[SW_browser] navegador web	**Riesgo**	**Tipo riego**	Riesgo Residual	Tipo de riesgo Residual
[E.1] Errores de los usuarios	2	Trivial	1,4	Trivial
[E.4] Errores de configuración	4	Trivial	2,8	Trivial
[E.8] Difusión de software dañino	15	Importante	10,5	Moderado
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.8] Difusión de software dañino	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas(software)	5	Tolerable	3,5	Trivial
[E.21] Errores de mantenimiento / actualización	4	Trivial	2,8	Trivial
[E.20] Vulnerabilidades de los programas (software)	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial

[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.11] Acceso no autorizado	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[Sw_email] servicios de correo	**Riesgo**	**Tipo riego**	**Riesgo Residual**	**Tipo de riesgo Residual**
[E.1] Errores de los usuarios	0	Trivial	0	Trivial
[E.4] Errores de configuración	2	Trivial	1,4	Trivial
[E.8] Difusión de software dañino	6	Tolerable	4,2	Trivial
[A.4] Manipulación de la configuración	2	Trivial	1,4	Trivial
[A.8] Difusión de software dañino	2	Trivial	1,4	Trivial
[E.20] Vulnerabilidades de los programas(software)	6	Tolerable	4,2	Trivial
[E.21] Errores de mantenimiento / actualización	2	Trivial	1,4	Trivial
[E.20] Vulnerabilidades de los programas (software)	2	Trivial	1,4	Trivial
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial

[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.11] Acceso no autorizado	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[Sw_office] Ofimática	**Riesgo**	**Tipo riego**	**Riesgo Residual**	**Tipo de riesgo Residual**
[E.1] Errores de los usuarios	2	Trivial	1,4	Trivial
[E.4] Errores de configuración	4	Trivial	2,8	Trivial
[E.8] Difusión de software dañino	15	Importante	10,5	Moderado
[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.8] Difusión de software dañino	5	Tolerable	3,5	Trivial
[E.20] Vulnerabilidades de los programas(software)	5	Tolerable	3,5	Trivial
[E.21] Errores de mantenimiento / actualización	4	Trivial	2,8	Trivial
[E.20] Vulnerabilidades de los programas (software)	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial

[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.11] Acceso no autorizado	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial
[SW_lengpro] lenguaje o plataforma de programación	**Riesgo**	**Tipo riego**	**Riesgo Residual**	**Tipo de riesgo Residual**
[E.1] Errores de los usuarios	0	Trivial	0	Trivial
[E.4] Errores de configuración	2	Trivial	1,4	Trivial
[E.8] Difusión de software dañino	6	Tolerable	4,2	Tolerable
[A.4] Manipulación de la configuración	2	Trivial	1,4	Trivial
[A.8] Difusión de software dañino	2	Trivial	1,4	Trivial
[E.20] Vulnerabilidades de los programas(software)	2	Trivial	1,4	Trivial
[E.21] Errores de mantenimiento / actualización	2	Trivial	1,4	Trivial
[E.20] Vulnerabilidades de los programas (software)	2	Trivial	1,4	Trivial
[A.5] Suplantación de la identidad del usuario	5	Tolerable	3,5	Trivial
[E.4] Errores de configuración	5	Tolerable	3,5	Trivial

[A.4] Manipulación de la configuración	5	Tolerable	3,5	Trivial
[A.11] Acceso no autorizado	5	Tolerable	3,5	Trivial
[A.5] Suplantación de la identidad del usuario	4	Trivial	2,8	Trivial

PROPUESTA DE PROYECTOS

Luego de realizar el análisis de gestión de riesgos a continuación se desarrollaran los proyectos que permitirán llevar a un nivel de riesgo aceptado ante un posible impacto de una amenaza materializada sobre un activo, los proyectos aprobados por la dirección se aplicaran sobre los riesgos importantes e intolerables que afectan a los activos que se detallaran a continuación.

ACTIVO	AMENAZA
[D_R] reservado	[E.19] Divulgación de información;
[D_L_Exa]Listado de examen	[E.19] Divulgación de información;
[S_Internet] Internet	[E.24] Caída del sistema por agotamiento de recursos
[S_Aten] Atención a la demanda educativa	[E.1] Errores de los usuarios
[S_Capacit] Servicio de capacitación y formación	[E.1] Errores de los usuarios
[Sw_office] Ofimática	[E.8] Difusión de software dañino
[SW_browser] navegador web	[E.8] Difusión de software dañino
[SW_dbms] sistemas de gestión de bases de datos	[E.8] Difusión de software dañino
[SW_os]sistemas operativos	[E.8] Difusión de software dañino
[SW_Aport] Aportes	[E.8] Difusión de software dañino

[SW_Tarant]tarantela nomina	[E.8] Difusión de software dañino
[SW_Cactus] Biodata	[E.8] Difusión de software dañino
[SW_Adm2000] Administración 2000	[E.8] Difusión de software dañino
[SW_SGVA] sistema de gestión virtual de aprendices	[E.8] Difusión de software dañino
SW_SAGC] sistema académico de gestión de centro	[E.8] Difusión de software dañino
[SW_web_regi] Pagina web de la regional Bolívar	[E.8] Difusión de software dañino
[SW_Spem] Servicio público de empleo	[E.8] Difusión de software dañino
[SW_Fin2000] Finanzas2000	[E.8] Difusión de software dañino

Los proyectos se definirán a nivel de gestión y a nivel técnico, los mismos lo encontraran en anexos Proyectos.xls

La programación de las actividades las podremos encontrar en el anexo Diagrama Gantt.

12. AUDITORIA DE CIMPLIMIENTO DE LA ISO: IEC 27002:2005

INTRODUCCION

A continuación se realizara una evaluación del nivel de cumplimiento respecto a los controles definidos por la norma ISO/IEC 27002:2005. Este análisis permitirá establecer aquellos controles que serán implementados por parte de la organización, aquellos que no y así determinar proyectos que mejoren la seguridad de la organización.

METODOLOGIA

Se definió que se utilizara el modelo de madurez de la capacidad CMM como metodología de análisis que evaluara el grado de madurez en la implementación del sgsi; este se basara en el ISO/IEC 27002:2005 el cual agrupa un total de 133 controles o salvaguardas, organizado en 11 áreas y 39 objetivos de control.

EVALUACION DE MADUREZ

El objetivo de esta fase es evaluar el nivel de madurez implementado en la seguridad en lo que respecta a los diferentes dominios de control y los 133 controles planteados por la Norma UNE-ISO/IEC 27001:2007, y los controles descriptos en la norma UNE-ISO/IEC 27002:2009.

Los dominios que deben analizarse son:

· Política de seguridad
· Organización de la seguridad de la información.
· Gestión de activos.
· Seguridad en los recursos humanos
· Seguridad física y ambiental
· Gestión de comunicaciones y operaciones.
· Control de acceso.
· Adquisición, desarrollo y mantenimiento de Sistemas de Información
· Gestión de incidentes
· Gestión de continuidad de negocio
· Cumplimiento

El estudio debe realizar una revisión de los 133 controles planteados por la norma para cumplir con los diferentes objetivos de control – el número de los cuales se indica entre paréntesis para cada uno de los dominios-. Esta estimación la realizaremos según la siguiente tabla, que se basa en el Modelo de Madurez de la Capacidad (CMM):

Como base de conocimiento se tomaran los siguientes valores:

EFECTIVIDAD	CMM	SIGNIFICADO	DESCRIPCIÓN
0%		Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
10%	**L1**	Inicial /Ad-hoc	Estado inicial donde el éxito de las actividades los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
50%	**L2**	Reproducible,perointuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método. No hay comunicación o entrenamiento formal, las responsabilidades que dan a cargo de cada individuo. Se depende del grado de conocimiento de cada individuo.
90%	**L3**	Procesodefinido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados mediante entrenamiento.
95%	**L4**	Gestionado y medible	Se puede seguir con indicadores numéricosy estadísticos la evolución de losprocesos.

			Se dispone de tecnología para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.
100%	**L5**	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos.

RESULTADOS

A continuación se presentan los resultados obtenidos luego de la auditoria de cumplimiento; los resultados abajo detallados reflejarán el grado de madurez del sistema especificado en la metodología CMM en función de cada control implementado de la norma UNE-ISO/IEC 27002:2009. Se realizó el mapeo de los 133 controles con el estado actual de la entidad, esto lo podremos encontrar en el Anexo 2 CMM.xls

A continuación se describe los controles implementados y el porcentaje de cumplimiento por cada dominio:

Dominio	Aprobados	NO Aprobados	Porcentaje Cumplimiento	CMM
Política de Seguridad Corporativa	2	0	0%	**L0**
Estructura Organizacional de Seguridad Informática	11	0	0%	**L0**
Clasificación y Control de Componentes Críticos	2	3	55%	**L2**
Seguridad del Recurso Humano	7	2	10%	**L1**

Seguridad Física y Ambiental	10	3	30%	**L1**
Administración de Operaciones y Comunicaciones	28	3	11%	**L1**
Control de Acceso	24	1	5%	**L0**
Desarrollo, Mantenimiento y adquisición de Sistemas de Información	16	0	0%	**L0**
Administración de Incidentes de Seguridad Informática	5	0	0%	**L0**
Administración de Continuidad del Negocio	5	0	0%	**L0**
Cumplimiento y Normatividad Legal	10	0	0%	**L0**

GRAFICOS NIVEL DE CUMPLIMIENTO

De acuerdo a los resultados arrojados, estos evidencian que la institución aprobó un alto número de controles ya que los que existían en el momento eran insuficientes para minimizar las amenazas existentes.

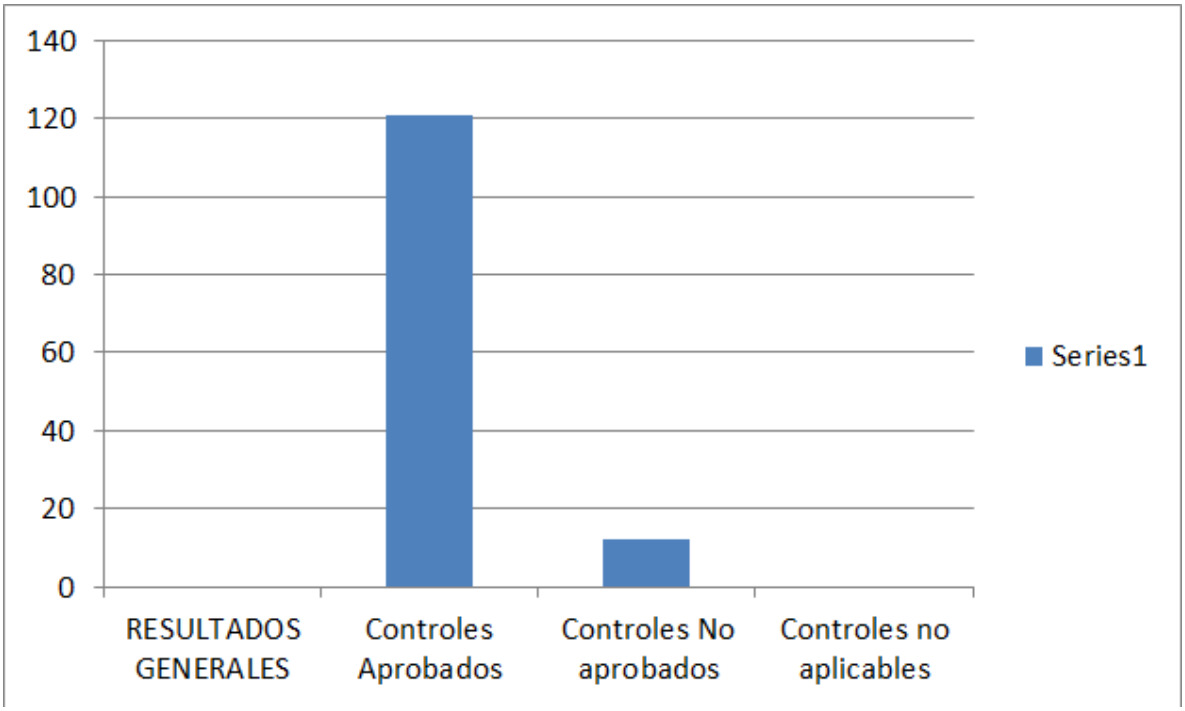


Figura 12.

En esta figura se detallan el porcentaje del nivel de cumplimiento para cada dominio de la ISO 27002.

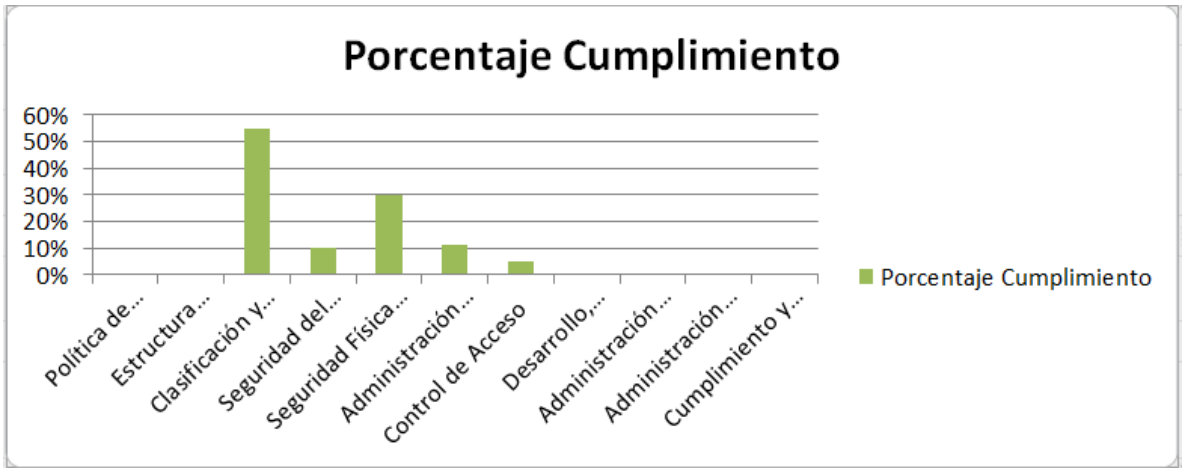


Figura 13.

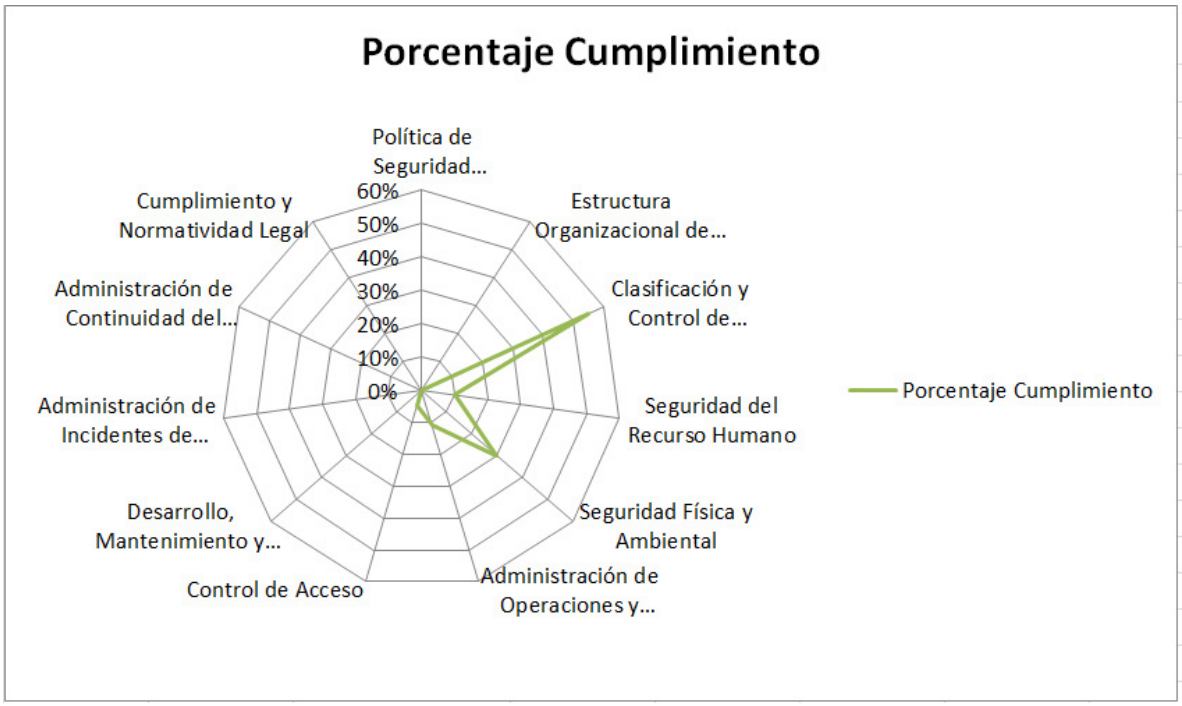


Figura 14.

REFERENCIAS BIBLIOGRAFICAS

http://www.iso27000.es/iso27000.html#section3b

http://www.iso27001standard.com/es/que-es-la-norma-iso-27001

http://iso27002.wiki.zoho.com/00-Cl%C3%A1usulas-ISO-27002.html

http://www.iso27000.es/download/doc_iso27000_all.pdf

http://auditoriauc20102mivi.wikispaces.com/file/view/NTCAS436020101700422184.pdf

http://www.innotecsystem.com/plandirectorseguridad.htm

http://blog.s21sec.com/2007/12/por-qu-un-plan-director-de-seguridad.html

http://www.sia.es/img/Plan_director_Cepsa-Sia.pdf

http://www.rediris.es/difusion/eventos/foros-seguridad/fs2010/pres/viiiforoseguridadRI2.pdf