**Asignatura:** Seguridad y Auditoría Informática

**Sección:** 371

**Nombre del docente:** Leighton Torres Carlos Alberto

**Nombre de los integrantes del grupo:** Ivo Olivares, Felipe Inda, Yerko Fuentes.

**Fecha de entrega:** 8 de abril de 2019

Problemática

identificación de riegos e impactos

**Empresa JetBlack LTDA.**

Contenido

[I. Introducción. 3](#_Toc5540720)

[II. Análisis riesgos sobre la infraestructura TI. 4](#_Toc5540721)

[III. Consecuencias de los ataques detectados. 8](#_Toc5540722)

[IV. Criterios de análisis establecidos y conceptos claves asociados. 8](#_Toc5540723)

[V. Supuestos determinan el propio punto de vista. 8](#_Toc5540724)

[VI. Conclusión 9](#_Toc5540725)

[VII. Referencias bibliográficas 9](#_Toc5540726)

Una vez finalizado el informe, actualiza esta tabla de contenidos, ubicando el mouse sobre ella, y pulsando el botón derecho del mouse. Actualízala en su totalidad y déjela en una página independiente de la Introducción. Finalmente elimina este texto.

1. Introducción.

A continuación, se realizará un análisis sobre la empresa **JETBLACK LTDA**, con el fin de identificar los todos los puntos de interés para una auditoria, esta empresa cuenta con giros en el área de tecnologías de la información y construcción de edificios, por lo que el análisis se centrará sobre los aspectos intrínsecos de estas industrias en las materias de vulnerabilidad y posibles mejoras en el modelo de negocio, todo desde un punto de vista externo y con la información que se a recopilado hasta la fecha.

*La empresa presenta problemas en el manejo de la información, tanto recursos digitales como en papel, presentando situaciones como:*

1. Perdida de información por mala manipulación.
2. Robo y venta de información.
3. Eliminación de datos de usuario desvinculados, comprometiendo la integridad de la base de datos.
4. Infección de servidores del centro jurídico, en una versión de Win Server 2008.  
     
   **El análisis incluirá:**

* Los activos vigentes identificados, tanto en materia de recursos humanos, monetarios tangible e intangible, y también tecnológicos.
* Matriz de riesgo con plan de acción para el actuar en situaciones de contingencia y para activos vulnerables.
* Identificación de los riesgos correspondientes a la industria TI.
* Identificación de los posibles ataques a los que está expuesta la organización.
* Análisis de impacto al negocio según los posibles ataques.
* Plan de recuperación ante desastres.
* Estrategias de recuperación y continuidad del negocio.
* Efecto de los ataques informáticos en la continuidad operacional y del negocio.

En modalidad de informe ejecutivo serán profundizadas los anteriores tópicos, las exigencias de calidad están centradas en los siguientes puntos:

* Correcto análisis sobre la infraestructura de TI
* Consideraciones sobre las consecuencias de los ataques detectados.
* Documentación de los ataques existentes a la seguridad informática.
* Correcto análisis general y conceptos clave asociados.
* Considerar supuestos correctos bajo un punto de vista de criterio experto.

Su principal función debe considerar:

* Incorporar estándares de calidad en materias TI y comunicación que permitan la mejora continua.
* Coordinar y velar por la integridad, confidencialidad y disponibilidad.
* Evaluar la incorporación de nuevas tecnologías e infraestructura TI.
* Orientar metodológicamente la identificación, elaboración y evaluación de proyectos informáticos.

1. Análisis riesgos sobre la infraestructura TI.
2. **Identifica los Activos de mayor impacto o críticos en la Organización.**

En este apartado, se identificarán los activos provenientes de la empresa JetBlack ya que presenta una problemática. En primera instancia debemos definir que es un Activo, cual son sus características y las clasificaciones de este.

Los Activos es un bien que la empresa posee y que puede convertirse en dinero u otros medios líquidos equivalentes, es decir, son ganancia mediante de un servicio, producto, entre otros.

Los activos que una empresa posee se clasifican dependiendo de su liquidez, es decir, la facilidad con la que ese activo puede convertirse en dinero. Por ello se dividen en:

1. **Activos tangibles**
   * Casa matriz de operaciones Región Metropolitana.
   * 4 sucursales: La Serena, Coquimbo, Ovalle y Tongoy.
   * Documentos legales de la institución.
   * Registro diario de la normativa asociada a contratos y proyectos.
   * Sistema de contabilidad de centro.
   * Políticas contables para que las cuentas operen bajo bases eficientes y consistentes.
   * Definición y asignación de responsabilidades de funcionarios y empleados.
   * Catálogo de cuentas y guía contabilizadora.
2. **Activos intangibles**

* Presta de servicios jurídicos en:
  + Elaborar y revisar la documentación de carácter legal en la institución. **(oficios, resoluciones, convenios, contratos, etc.)**
  + Elaborar el registro diario de la normativa vinculada a Contratos y Proyectos, publicada en el Diario Oficial.
  + Asesorar a la Secretaría en asuntos legales en que tenga participación la institución.
  + Atender consultas de las áreas técnicas de las áreas tecnológicas, contables y de Edificación.
* Presta de servicios contables en:
  + Establecer y operar las medidas necesarias para garantizar que el sistema de contabilidad del Centro este diseñado para que su operación facilite la fiscalización de los activos, pasivos, ingresos, costos y gastos de la organización.
  + Realizar las acciones necesarias para garantizar que el sistema contable del organismo, así como las modificaciones que se generen por motivos de su actualización, cuenten con las autorizaciones legales para su funcionamiento y operación.
  + Llevar a cabo la contabilidad del Centro en los términos que establece la Ley de Presupuesto, Contabilidad y Gasto Público.
  + Emitir por escrito las principales políticas contables necesarias para asegurar que las cuentas se operen bajo bases eficientes y consistentes, así como para la clara definición y asignación de responsabilidades de funcionarios y empleados.
  + Emitir por escrito las principales políticas contables necesarias para asegurar que las cuentas se operen bajo bases eficientes y consistentes, así como para la clara definición y asignación de responsabilidades de funcionarios y empleados.
  + Registrar y controlar los recursos financieros provenientes del calendario financiero presupuestal, los que otorgan las instituciones para el desarrollo de proyectos de investigación, así como los ingresos de donativos provenientes de dependencias y entidades del sector público, privado o social, identificando dentro de la contabilidad, los recursos aportados por instituciones públicas y privadas, destinados a proyectos específicos.
  + Elaborar, analizar y consolidar los Estados Financieros del Centro y de las Unidades Foráneas.
* Presta de servicios tecnológicos en:
  + Desarrollo de Sistemas. Analizar, diseñar y desarrollar los sistemas informáticos y supervisar aquellos que son de responsabilidad de contrapartes externas.
  + Desarrollo de Sistemas. Analizar, diseñar y desarrollar los sistemas informáticos y supervisar aquellos que son de responsabilidad de contrapartes externas.
  + Entrega de servicios electrónicos **(PC, correos, internet, software, etc.)**. Administrar y asegurar la disponibilidad de las redes, comunicación, servidores y estaciones de trabajo.
  + Investigaciones e innovación de tecnología. Buscar y proponer nuevas herramientas o estándares tecnológicos que aporten al desarrollo institucional en términos de mejoras en los procesos del Servicio.
  + Servicios Importantes con los que cuenta la Organización y son responsabilidad del Área. Servidor Documental de Jurídico, Servidor de Sistema SAP, Servidor de Dominio, Servidor de Intranet y Servidor de Correo.

***Esta área cuenta con subdivisiones de especialidades que están conformadas por distintos expertos en el área, su enumeración y función a continuación:***

1. Unidad de desarrollo:
   * Administra las redes y servicios de telecomunicaciones.
   * Mantención de la seguridad en la red.
   * Mantención y administración a los servidores de documentos jurídicos, servidor de sistema SAP, servidor de dominio, servidor de intranet y de correo.
   * Respaldo de información.
2. Unidad de soporte:
   * Mantenimiento correctivo sobre hardware y software.
   * Soporte a todas las sucursales tanto en terreno como mediante telecomunicaciones.
   * Recepción de hardware con fallas.
   * Instalación de software en casos necesarios.
3. **Activos humanos**

* 300 funcionarios con 100 flotantes por año.
* Trabajadores de planta.
* Trabajadores a contrata.
* Trabajadores Honorarios.
  + Departamento de jurídico.
  + Departamento de contabilidad y finanzas.
  + Departamento de TI.
    - Unidad de desarrollo.
    - Unidad de sistemas.
    - Unidad de soporte.

1. **Identifica los riegos a los que están expuestos los Activos de la Organización.**
2. **Identifica los tipos de Ataques a los que se encuentra expuesta la Organización.**

En este apartado se definirá los tipos de ataques que existen según la Metodología Magerit, el cual dice que existen los siguientes tipos.

* + **No intencional**
  + **Desastre Natural**
  + **Planificado o Intencional**
  + **Hacker o Hacking**

Se definirán cada uno de ellos y después se identificarán con una justificación.

* + **No intencional:** Ataque no propuesto por una persona o grupo natural en cual se efectúa por una acción determinada.
  + **Desastre Natural:** Ataque propuesto por fenómenos naturales, tales como: terremoto, maremoto, huracanes, entre otros.
  + **Planificado o Intencional:** Ataque propuesto por una persona o grupo natural en cual se efectúa por una acción determinada.
  + **Hacker o Hacking:** Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos. Entre los ataques de Hacking existen estos cuatro más importantes.
    - * 1. **DoS:** un atacante intenta evitar la legitimidad de que los usuarios accedan a información o a los servicios.
        2. **Ping Flood:** se basa en enviar a la víctima una cantidad abrumadora de paquetes ping, lo cual fuerza al sistema a colapsar.
        3. **Ping de la muerte:** El atacante envía un paquete ICMP de más de 65.536 bytes. Como el sistema operativo no sabe cómo manejar un paquete tan grande, se congela o se cuelga en el momento de volver a montarlo.
        4. **Ataque Man-In-The-Middle:** Un ataque MITM ocurre cuando una comunicación entre dos sistemas es interceptada por una entidad externa.

**Posibles ataques hacia a la empresa JetBlack.**

Uno de los ataques que descastamos como grupo de trabajo **son los desastres naturales y No intencionales**, que ya es uno de los pocos ataques que no afectaría a mayor escala si llegase a ocurrir en un momento cualquiera, cabe a destacar que se mantiene en una prioridad baja como amenaza.

**El ataque de prioridad mediana son los planificados o intencionales**, ya que se puede percibir mediante la vista de comportamiento de las personas y mitigarse como gente que tenga conocimiento sobre movimientos de organizaciones o que ya haya participado en una actividad ilícita y prestas sus servicios para ayudar a la empresa.

**Los ataques de prioridad superior son los Hacker o Hacking**, ya que afecta directamente en el sistema de la empresa, los cuales manejan información exclusiva de la empresa y cualquier mal entendió puede dañar la integridad de la empresa y sus usuarios. Este ataque se ve directamente proporcional al servidor con la documentación, programas y/u otro tipo de archivo que maneje la empresa.

1. Consecuencias de los ataques detectados.
2. Construye Matriz de Riesgo, identificando el Activo o Servicio Expuesto en función de la Probabilidad e Impacto de que ocurra un ataque.
3. Criterios de análisis establecidos y conceptos claves asociados.
4. Realiza el Análisis de impacto al negocio en función de la probabilidad que ocurra un ataque en la Organización.
5. Supuestos determinan el propio punto de vista.
6. Realiza un Plan de recuperación ante desastre para cada Activo o Servicio que pueda ser Atacado.
7. Desarrolla estrategias de recuperación y continuidad del negocio para cada Activo o Servicio que pueda haber sido afectado.
8. Conclusión

1. Referencias bibliográficas

*Rubén Marino (2018).* *Vulnerabilidades Y Ataques Informáticos: Tipos de ataques informáticos y cómo prevenirlos. Recuperado de* <https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/>

*Libros de Metodología Magerit (2012). Metodología Magerit: Libro I – Método. Recuperado de Material de apoyo propuesto por el Docente.*

*Libros de Metodología Magerit (2012). Metodología Magerit: Libro II - Catálogo de Elementos. Recuperado de Material de apoyo propuesto por el Docente.*