**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.**

El análisis de riesgos informáticos debe contener la identificación de los activos informáticos, sus vulnerabilidades y amenazas a las que son vulnerables, la probabilidad y el impacto de estas mismas.

La principal motivación de esto es que la explotación de algún riesgo representaría daños o pérdidas financieras o administrativas, por lo que se debe tener en cuenta los problemas a los que se enfrenta en esta situación, estimar la magnitud y colocar los controles para que sean efectivos, para que dichos controles sean efectivos deben ser implementados en un arquitectura conjunta de seguridad, con la finalidad de preservar las propiedades de confidencialidad integridad y disponibilidad de los recurso objetos de riesgo.

Con la intensa competencia que se vive hoy debido al efecto acelerador de las TI, las empresas invierten en maneras de integrar las TI a la lógica del negocio sin temor a ser alcanzados por los riesgos.

El aumento del uso de dispositivos móviles ha supuesto una mayor vulnerabilidad al momento del almacenamiento y la transferencia de datos.

**Principios en la gestión de activos para la gestión de riesgos:**

* Los activos existen para generar valor a la organización y sus accionistas.
* La gestión de los activos transforma la política den decisiones técnicas y financieras, planes y actividades.
* La gestión de los activos asegura el cumplimiento de sus funciones y la consecución de los objetivos estratégicos.
* Liderazgo y cultura son determinantes en la realización de valor.

Sobre lo anterior, la triada de desarrollo es coste riesgo y desempeño, por lo que se debe considerar estas tres variables al momento de la planeación.

- Integridad: Riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamientos y reportes de las aplicaciones utilizadas en una organización.

• Interfaz del usuario: Relacionado con las ejecuciones de un sistema o negocio.  
 • Procesamiento: Relacionado con que haya controles correctivos y preventivos sobre la exactitud e integridad de los datos.  
 • Procesamiento de errores: Relacionado con los controles sobre el procesamiento de la información.  
 • Interfaz: La información ha sido procesada y transmitida adecuadamente  
 • Administración de cambios  
 • Información

- Relación: Uso oportuno de la información creada por una aplicación, esto se relaciona con la toma de decisiones.

- Acceso: Hace referencia al inapropiado acceso a los sistemas, datos e información. Hace referencia a la disponibilidad, confidencialidad y integridad de los datos considerando los siguientes puntos.

• Procesos de negocio  
 • Aplicación  
 • Administración de la información  
 • Entorno de procesamiento  
 • Redes  
 • Nivel físico

- Infraestructura: No exista una estructura de información tecnológica efectiva en la organización para soportar adecuadamente las necesidades futuras y presentes de los negocios, entre ellas se encuentran

• Planeación organizacional  
 • Definición de las aplicaciones  
 • Administración de seguridad  
 • Operaciones de red y computacionales  
 • Administración de sistemas de bases de datos  
 • Información / Negocio

- Seguridad General: Los estándares IEC 950 proporcionan los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo:

•Riesgos de choque de eléctrico: Niveles altos de voltaje.  
 •Riesgos de incendio: Inflamabilidad de materiales.  
 •Riesgos de niveles inadecuados de energía eléctrica.  
 •Riesgos de radiaciones: Ondas de ruido, de láser y ultrasónicas.  
 •Riesgos mecánicos: Inestabilidad de las piezas eléctricas

- Procesamientos más grandes y complejos  
- Dependencia del personal clave

Identificación de tipos de riesgos relevantes

-Riesgo País  
-Riesgo Organizacional  
-Riesgo de negocio  
-Riesgo Tecnológico  
-Riesgo Operacional  
-Riesgo Informático

***Controles recomendados para el acceso a la red:***

1. Control en la conexión a la red con subredes con las siguientes distinciones:
   1. **Red de usuarios:** Preparada con un entorno sandbox para usuarios externos que por motivos de contingencia requieran accesos a la red.
   2. **Red de trabajadores:** Preparada como red de alto rendimiento y servidor Windows Server 2016 con Active Directory para el control de roles y usuarios, como medida adicional realizar la validación por MAC Address de equipos.
   3. **Red administrativa:** Red oculta que contiene todos los permisos, se realizara validación mediante MAC Address a los equipos y una clave única de 4 dígitos.

La idea general de estos controles es restringir el acceso en la mayor medida posible y además de estos, poder identificar a la brevedad a los trabajadores que se vean involucrados en situaciones de falta.

***Controles recomendados para la manipulación de documentos jurídicos:***

La primera recomendación respecto al control sobre documentos jurídicos es lograr una migración completa de los sistemas hacia las firmas digitales, con contratos inteligentes.

A posteriori no se necesitaría tener un servidor dedicado, con todos los contratos ya logrados en materia de seguridad y fiabilidad.

***Controles recomendados para el control de la información:***

En conjunto con las restricciones de accesos a la red proporcionados por Windows Server, se debe agregar un trackeo al movimiento de los usuarios dentro de los roles con manejo de información sensible, con el fin de saber si algún trabajador incurre en mala praxis, los castigos en este caso deben ser proporcionados por el área de gobierno en la empresa.

Para completar mas este apartado, se agregará una matriz de riesgo con casos de estudio más diluidos:

|  |
| --- |
|  |

1. **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. Criterios de análisis establecidos y conceptos claves asociados.

En el negocio, la probabilidad de ataque físico es verdaderamente baja en relación con ataques informáticos, pero cada cual tiene su posibilidad de ocurrir:

**Un ataque** representa tiempo de **Down time** para el negocio, por lo que, dependiendo de su gravedad, el negocio puede **quedar fuera del mercado por un tiempo importante**, castigando la negligencia en los sistemas con recursos de tiempo, humanos y monetarios, que se deben invertir para volver a poner en marcha la empresa.

Otro tipo de siniestro es **el robo de información**, este es mucho más difícil de identificar sin los controles adecuados, por lo que es indispensable contar con ellos. En el caso de que los rivales en la industria obtengan la data, podrían tomar contacto con los clientes sin problemas, y basándose en las transacciones, saber cuanto es el precio correcto para realizar buenas ofertas, además que contarían con toda la estructura pensada para ser una ventaja competitiva, y se perdería todo esto por la venta ilegal de información.

Los **ataques físicos** corresponden a la capa mas primitiva como vector de ataque, también la más improbable, pero a su vez una de las mas perjudiciales. Dependiendo de que tan profundo es el alcance del ataque, puede ser desde **perdidas leves en materiales sin importancia hasta una perdida total de la infraestructura de trabajo**, por lo que los controles físicos si bien son necesarios, representar mas una buena practica dentro del ambiente, además que la correcta función de los controles físicos también previenen el robo de información por parte de trabajadores sin accesos a los servidores pero que poseen interfaces de conexión para obtener la data.

En materia de continuidad de negocio, lo mas perjudicial es un ataque físico con un profundo alcance, pudiendo incluso destruir toda la inteligencia conseguida con mucho trabajo, aunque como se mencionaba anteriormente, es el tipo de ataque menos común.

1. Supuestos determinan el propio punto de vista.

Plan de recuperación para desastres:

1. ***Mala manipulación de datos:***  
   Para la correcta aplicación de este plan de contingencia, se debió tener en cuenta la aplicación de los llamados Smart Contracts, en tal caso, la infraestructura esta diseñada para mantener la integridad de los datos incluso en las peores catástrofes, colocando un servidor de respaldo como una medida innecesaria.
2. ***Robo y venta de datos:***  
   La primera acción a ejecutar es, mediante el sistema de traqueo previamente recomendado, identificar al usuario que ha movido los documentos de manera ilícita, proceder a denunciarlo a la justicia mediante el procedimiento correspondiente, luego de eso, identificar mediante los medios lícitos al alcance de la mano a la organización coludida en la compra de información privilegiada, en caso fructífero realizar la denuncia correspondiente, identificar el vector de ataque que permitió esta falencia en la seguridad y modelar controles que puedan solventar esta situación.
3. ***Infección de servidores con malware:***  
   Identificar el tipo de ataque y realizar las funciones de limpieza correspondientes, si es posible identificar el medio de infección se debe trazar el vector de ataque y modelar los controles necesarios para su pronta integración al sistema y mantener estos ataques al mínimo, se debe considerar que gran parte de la internet contiene malware, así que es probable que esto suceda en reiteradas ocasiones.
4. ***Caída del sistema de contabilidad:***  
   Debido a la importancia del servicio que proporciona el sistema de contabilidad, seria una buena idea mantener un servidor espejo que contenga copias de la BD y otros documentos en tiempo real, con el fin de reestablecer el servicio a la brevedad luego de la caída, posterior a la solución, identificar el motivo de la caída del servidor y proceder a su reparación por parte del equipo de tecnología.
5. ***Actualizaciones defectuosas del sistema de contabilidad:***  
   Se debe mantener un repositorio privado entre los desarrolladores con las distintas versiones de código estable, por lo que su restitución no debería representar un problema.
6. ***Incoherencias en el catalogo de cuentas y guía contabilizadora:***  
   Se debe recurrir a una corrección de los valores cuestionados, mediante horas hombre de trabajo, o en su defecto horas maquina de trabajo, seria correcto realizar una comparación entre los procedimientos utilizados por cada cual y sus resultados.
7. ***Caída en las telecomunicaciones:***Identificación de la causa de caída, para este efecto se puede recurrir al proveedor de internet, dependiendo de la causa, se deberá tomar la determinación de esperar una solución por parte del ISP o el equipo tecnológico ser el encargado de la corrección.
8. ***Caída en los servidores:***En la caída de los servidores puede haber múltiples actores involucrados, por lo que es crucial habilitar la función log de errores de sistema, o en su defecto, un trackeo de las funciones conflictivas mediante distintos métodos de control, una vez identificada la problemática, el equipo de tecnologías debe procede a la reparación.
9. ***Falla en equipos de trabajo:***  
   Esta falla es relativamente común, el procedimiento adecuado sería el retirar el equipo del su trabajador, entregarle otro equipo, y proceder a su evaluación y si es posible su reparación, es importante identificar la causa de la falla, si es por negligencia o no, con el fin de endosar las obligaciones monetarias del caso al usuario del equipo, en caso contrario proceder a su reposición sin costo.
10. ***Ataques informáticos:***  
    Puede representar una amenaza realmente seria, considerando las posibilidades de robo de datos y destrucción de activos informáticos, una alternativa loable para la continuidad del negocio es la construcción de un servidor espejo, con la misma información disponible en el servidor principal, con el fin de reestablecer las operaciones en un reducido periodo de tiempo, y además de esto, en caso de falla critica con perdida de datos por el servidor, se conservarían estos mismos sin problemas latentes de ninguna índole.

Lo anterior corresponde a la respuesta a posibles ataques de distinta índole, el fin de su representación es poder estar preparado en caso de la realización de estos ataques y poder continuar con las operaciones del negocio, con la calidad competitiva adecuada al caso.

1. Conclusión

Como conclusión podemos extraer la cantidad de riesgos asociados a la industria de la tecnología, tanto en el ámbito de su utilización por usuarios bien intencionados como mal intencionados, por lo que es menester poseer los controles de seguridad apropiados para el correcto funcionamiento de esta arquitectura empresarial, considerando que la mayor cantidad de procesos clave pasan sin lugar a duda por estas formas de aceleración.

La competitividad de una empresa se ve seriamente comprometida en cuanto a su uso de tecnologías de la información, por lo que representan una clara ventaja competitiva con respecto al mercado, en caos de usarse correctamente, en casos de mal versación, puede paralizar una empresa o hacerla perder valiosos recursos en una cantidad mínima de tiempo.

Es necesario que el área de tecnología cuente con los planes de contingencia adecuados para la correcta solvencia de estas situaciones, por lo que un área especializada dentro del departamento seria un gran aporte a la seguridad de los procesos, la eficacia y la eficiencia de estos, porque se debe recordad que, dentro del ámbito de ejecución de controles, también se busca la mejora en la calidad de las operaciones de bajo y alto nivel.

Casos como la malversación de información por parte de trabajadores es mucho más común que lo que cabría pensar, y además por cualquier clase de motivo irrelevante, por lo que mantener siempre los ojos sobre los controles es un punto a favor en la prevención de perdidas.

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.*

Recuperado para análisis de riesgos sobre la organización: https://es.scribd.com/doc/29676926/RIESGOS-INFORMATICOS