  
**FACULTAD DE ARQUITECTURA E INGENIERIA  
Plan de Trabajo de investigación titulado:**

Implementación de un procedimiento de diagnostico continuo y mitigacion de riesgos para la Empresa Tatoo Adventure Gear.

**Realizado por:**

Wágner Alexander Cadena Lastra

**Director del proyecto:**

Ing. Verónica Rodríguez Arboleda, MBA.

Como requisito para la aprobación de la materia:  
DESARROLLO DEL PROYECTO DE INVESTIGACIÓN   
MAESTRIA EN CIBERSEGURIDAD

QUITO, septiembre 2019

Nota del autor

[Incluya información sobre becas o ayudas y una dirección postal completa.]

Resumen

[El resumen ha de tener una longitud de un párrafo de entre 150 y 250 palabras. sin sangría. Los títulos de sección, como la palabra Resumen anterior, no se consideran títulos, por lo que no se usa formato de título en negrita. En su lugar, use el estilo Título de sección. Este estilo inicia automáticamente la sección en una nueva página, por lo que no es necesario que agregue saltos de página. Tenga en cuenta que todos los estilos de esta plantilla están disponibles en la pestaña Inicio de la cinta, en la galería de estilos.]

Palabras clave: [Haga clic aquí para agregar palabras clave.]

Implementación de un procedimiento de diagnostico continuo y mitigacion de riesgos para la Empresa Tatoo Adventure Gear.

# El Problema de investigación

## Planteamiento del problema

### Diagnostico.

Tatoo Adventure Gear ha crecido durante el último año incorporando a sus servicios dos nuevas innovaciones de negocios, uno es el mejoramiento de su sitio web representado por la optimización de su sistema y la segunda ampliación del catálogo de servicios con la incorporación de paquetes turísticos que se pueden contratar en un sitio web independiente y dedicado.

No se ha realizado una auditoria de sistemas y de seguridad en los últimos 3 años, por lo que ahora se desea conocer el estado del área informática y cuáles son las oportunidades de desarrollo potenciales que por la falta de documentación están ocultos.

El área de sistemas no cuenta con políticas de seguridad de la información,el área de desarrollo web, el área de desarrollo de ERP y Helpdesk cuentan con procedimientos, los cuales ahora no son suficientes, y las reglas de antivirus se pueden complementar con políticas de usuarios, esta es una oportunidad de mejora importante.

Es menester que al crecer las empresas busquen facilidades para conocer, catalogar y planificar el manejo de sus activos tecnológicos, el manejo de contabilidad sobre los activos generalmente incluye información de la fecha de compra, importante para el manejo de devaluación, modelos y proveedores, relevante para las garantías y el código contable, importante para el momento de realizar un levantamiento contable, sin embargo, ninguno estos datos ayudan al saber si estos activos están aportando al cambio tecnológico, o si se están cumpliendo las normativas sobre el uso de licencias o si se está aprovechando al 100% los equipos que tiene la empresa.

Uno de las responsabilidades del equipo de Helpdesk se centran en la protección de los sistemas electrónicos, y la primordial garantía de seguridad en la que confían se centra en el antivirus, pero no se toma en cuenta la seguridad física al momento de crear una protección general a los riesgos de la organización, las paredes, cerraduras son un factor importante en la seguridad, pero no es suficiente, políticas, control de inventarios, control de software y control de permisos son necesarios.

En contraste, es más fácil enseñarle a un ingeniero informático o eléctrico las bases de la seguridad física que a otra persona con un grado de capacitación diferente enseñarle bases de seguridad digital, razón por la cual las interacciones entre la protección física y lógica generalmente dependen de la persona de sistemas para administrar.

Ahora debemos tener en cuenta que muchos mecanismos de seguridad de la información pueden ser derrotados sin la necesidad de la intervención física de un “chico malo” ya sea en el desarrollo, durante el envío o la instalación de software, ya que un usuario bien intencionado podría “Sin querer” dar acceso a la infraestructura o a datos de la empresa al instalar un programa no catalogado y que puede tener vulnerabilidades.

Además, la empresa entiende que dar facilidades a los usuarios para que conecten sus equipos particulares a la red y puedan comunicarse con proveedores, compañeros y familiares por medio de la tan galopante nueva mensajería como es WhatsApp les da tranquilidad, ahorro y con un nuevo concepto que es el salario emocional, sin embargo, esto genera un nuevo reto al equipo de sistemas ya que deben determinar cuáles equipos deben tener acceso y cuales pertenecen a la organización y cuáles no.

Se ha realizado una auditoria y la observación directa muestran que la organización no cuenta con un manual de políticas de tecnologías, tampoco manual de procedimientos de tecnología y ni planes de contingencia, y existen brechas en la seguridad tales como:

* La organización no cuenta con un sistema de Directorio Activo, que permita implementar controles óptimos para gestionar el acceso y el uso controlado de los recursos de la red de datos corporativa.
* A pesar de que la organización cuenta con un antivirus corporativo debidamente licenciado, existen equipos que no están protegidos con esta herramienta.
* Existen usuarios que no hacen uso del bloqueo de pantallas en los ordenadores asignados, esto permite que cualquier persona pueda acceder a ellos cuando el usuario se ausenta de su lugar de trabajo.
* Las credenciales de las cuentas de correos electrónicos de los usuarios son conocidas por los administradores de tecnología.
* No existe puerta metálica ni con panel biométrico en el acceso al centro de cómputo.
* Se evidencia que existe una deficiencia con el control de acceso a periféricos como USB, esto permitiría la infección del equipo por malware o la sustracción de información.
* No existen convenios de confidencialidad para las personas que ocupan cargos críticos en donde se establezcan cláusulas de no divulgación de información de la organización.
* El área de tecnología no posee una política de seguridad informática donde se detallen los lineamientos y responsabilidades para el tratamiento seguro de la información, poniendo en riesgo a la confidencialidad, integridad y disponibilidad de esta.

### Pronostico.

Tatoo Adventure Gear ha determinado como parte de su estrategia institucional la innovación dentro del área deportiva, optimizando su catálogo de servicios e invirtiendo en Innovación y desarrollo (I+D), debido a esta nueva estrategia es importante considerar como prioridad la seguridad de la información, que es uno de los activos valiosos que garantizan continuidad del negocio y sostenibilidad a la organización.

Tabla : Crecimiento de población institucional.

|  |  |  |
| --- | --- | --- |
| Año | Cantidad de ingresos de usuarios por año. | Crecimiento del personal al año. |
| 2015 | 3 | 30 |
| 2016 | 2 | 32 |
| 2017 | 2 | 34 |
| 2018 | 3 | 37 |
| 2019 | 3 | 40 |

Fuente: Área de contabilidad Tatoo.

Tabla : Crecimiento de Ventas por año

|  |  |
| --- | --- |
| Año | Porcentaje de incremento en ventas |
| 2015 | 45 |
| 2016 | 55 |
| 2017 | 59 |
| 2018 | 62 |
| 2019 | 63 |

Fuente: Área de Ventas y Marketing.

Como podemos observar la cantidad de ventas y de usuarios ha tenido un crecimiento importante para la empresa, de la mano de este crecimiento los equipos y software también han aumentado, causando el cambio de la infraestructura incluso de ubicación de las oficinas, esto naturalmente ha elevado los requerimientos de seguridad en el área de Helpdesk, siendo imprescindible la implementación de políticas de seguridad a la medida, estas políticas tiene la labor de evitar en lo posible daños, la perdida de reputación de la empresa, perdidas económicas y afectación de productividad.

En contraste se necesita colocar un grupo de controles sin afectar la eficiencia, el grado de colaboración, utilidad, productividad o los fondos y recursos pertinentes, la alta directiva ha determinado que desea una solución de seguridad informática, pero sin que el tiempo que se dedique a ello retrase los lanzamientos de Innovación y desarrollo, tampoco que consuma los recursos asignados a las principales prioridades de innovación y que tampoco signifique incrementos en los costos, así que se va a planear usar una herramienta que se adapte a esta necesidad inicial.

### Control de pronostico

Es necesario proporcionar un método para evaluar el riesgo mediante el cálculo de la probabilidad de un impacto para la empresa, los clientes, los objetivos comerciales y las entidades externas (reguladores, proveedores, etc.). y que se mantenga en el marco de lo que vamos a denominar como riesgo razonable, el cual generara un plan de “seguridad razonable”.

CIS RAM proporciona un método para "trazar una línea" en la definición de riesgo aceptable de una organización, con riesgos por debajo de la línea que se adhieren a la atención debida y riesgos por encima de la línea que requieren tratamiento de riesgo.

Referencias

Apellidos, n. s. (Año). Título del artículo. *Título del diario*, Páginas desde - hasta.

Apellidos, n. s. (Año). *Título del libro.* Nombre de la ciudad: Nombre del editor.

Notas al pie

1[Agregue notas al pie, si corresponde, en su propia página después de las referencias. Para los requisitos de formato de APA, simplemente escriba sus propias referencias y notas al pie. Para dar formato a una referencia de nota al pie, seleccione el número y, después, en la Galería de estilos de la pestaña Inicio, haga clic en Referencia de nota al pie. En el cuerpo de una nota al pie, como en este ejemplo,se usa el estilo de texto Normal. (Nota: Si elimina esta nota al pie de ejemplo, no se olvide de eliminartambién su referencia en el texto. Está al final del párrafo Título 2 de ejemplo de la primera página del contenido del cuerpo de esta plantilla).]

Tablas

Tabla 1

[Título de tabla]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Encabezado de columna | Encabezado de columna | Encabezado de columna | Encabezado de columna | Encabezado de columna |
| Encabezado de fila | 123 | 123 | 123 | 123 |
| Encabezado de fila | 456 | 456 | 456 | 456 |
| Encabezado de fila | 789 | 789 | 789 | 789 |
| Encabezado de fila | 123 | 123 | 123 | 123 |
| Encabezado de fila | 456 | 456 | 456 | 456 |
| Encabezado de fila | 789 | 789 | 789 | 789 |

Nota: [Coloque todas las tablas del artículo en una sección de tablas, después de las referencias (y, si corresponde, de las notas al pie). Use una página nueva para cada tabla e incluya un número de tabla y un título de tablapara cada una, como se muestra en esta página. Todo el texto explicativo aparece en una nota de tabla después de la tabla, como en esta. Use el estilo de tabla o ilustración, disponible en la galería de estilos de la pestaña Inicio, para agregar el espaciado entre la tabla y la nota Las tablas en el formato de APA pueden usar un interlineado de una línea o de 1,5 líneas. Incluya un título para cada fila o columna, incluso si el contenido parece obvio. Se configuró un estilo de tabla predeterminado para esta plantilla que cumple con las normas del estilo APA. Para insertar una tabla, en la pestaña Insertar, haga clic en Tabla.]

Título de ilustraciones

Ilustración 1. [Incluya todas las ilustraciones en su propia sección, después de las referencias (y, si corresponde, de las notas al pie y las tablas). Incluya un título numerado para cada ilustración. Use el estilo de tabla o ilustración para agregar fácilmente espaciado entre la ilustración y el título.]

Para obtener más información sobre todos los elementos del formato de estilo APA, vea el Manual de estilo de la APA, 6.ª edición.