UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS “ESPOG”

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: **RPC-SO-02-No.053-2021**

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del artículo
PROPUESTA DE ESTRATEGIA PARA EVITAR LA FUGA DE INFORMACIÓN EN EMPRESAS CONSTRUCTORAS UTILIZANDO DETECCIÓN POR COMPORTAMIENTO (UEBA) CASO DE ESTUDIO: SCMI INC (USA)
Línea de Investigación:
SEGURIDAD INFORMÁTICA
Campo amplio de conocimiento:
TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Autor:
Wilmer Xavier Angulo Cárdenas
Tutor:
MSc. Pablo Marcel Recalde Varela

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, MSc. Pablo Marcel Recalde Varela con C.I: 171168505-5 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de estrategia para evitar la fuga de información en empresas constructoras utilizando detección por comportamiento (UEBA) caso de estudio: SCMI INC (USA)

Elaborado por: Wilmer Xavier Angulo Cárdenas, de C.I:0400987087 estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Universidad Israel

Yo, Wilmer Xavier Angulo Cárdenas con C.I: 0400987087, autor/a del proyecto de titulación denominado: Propuesta de estrategia para evitar la fuga de información en empresas constructoras utilizando detección por comportamiento (UEBA) caso de estudio: SCMI INC (USA). Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., febrero de 2023

Firma

ORCID: 0000-0002-6760-156X

Tabla de contenidos

APROBACIÓN DEL TUTOR 2
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE 3
INFORMACIÓN GENERAL 7
Contextualización del tema 7
Problema de investigación 8
Objetivo general 8
Objetivos específicos 8
Vinculación con la sociedad y beneficiarios directos: 8
CAPÍTULO II: ARTÍCULO PROFESIONAL 21
CONCLUSIONES 28
RECOMENDACIONES 29
BIBLIOGRAFÍA 30

Índice de tablas

Tabla 1 Clasificación de la información 13
Tabla 2 Objetivos de la seguridad de la información 14
Tabla 3 Factores comunes de fuga de información 16
Tabla 4 Ventajas y Desventajas de herramientas UEBA 19
Tabla 5 Comparativa de Herramientas UEBA 20

Índice de figuras

Fig 1 Objetivos seguridad de la información 14
Fig 2 Principales empresas EPC en Ecuador 18

INFORMACIÓN GENERAL

Contextualización del tema

La información constituye el activo más importante que tiene una organización. En muchos casos es considerada el activo principal. La ausencia de esta provoca que las empresas no puedan realizar eficientemente su trabajo. Llega a ser más importante que los elementos físicos como pueden ser sus instalaciones. Proteger la información involucra muchos actores, actividades y responsables, pues los datos correctamente asegurados ayudan a las organizaciones a crecer y mantenerse activas inclusive con la ausencia de instalaciones o luego de algún incidente que comprometa estas. (José Manuel Rovirata - INCIBE, 2021)

La acción de proteger la información implica tener en cuenta tres propiedades principales que son: confidencialidad, integridad y disponibilidad. El proceso de fuga de información se refiere a la pérdida de la confidencialidad, esto puede provocar que dicha información que debería ser solo conocida por un grupo de personas en la empresa, sea visible o pueda ser accesible para personas que no deberían hacerlo. (Revista UNIR, 2020)

Con el transcurrir del tiempo y el vertiginoso avance tecnológico, las amenazas también han evolucionado y se han identificado dos orígenes principales de estas: el origen interno que tiene que ver con los incidentes de seguridad provocados por personal de las propias organizaciones y el de origen externo que es provocado por ataques cuyo objetivo es conseguir rédito económico o dañar la imagen de la empresa (Yulima Hernandez, 2022)

Acorde a InsightExpress (2018) a pesar de que la organización haya elaborado políticas o procedimientos en cuanto a la seguridad, existen conductas arriesgadas que ponen en peligro la información empresarial como la personal. Dichas conductas podrían ser:

- Uso de software no autorizado
- Uso de computadores de la organización para trabajos personales
- Permitir el acceder a la red de la empresa a gente no autorizada
- Uso no adecuado de claves o compartir estas con otras personas

Este documento plantea la definición una estrategia que permita identificar y posteriormente mitigar el riesgo asociado con la fuga de datos. Además, se tiene como objetivo el análisis de las herramientas User and Entity Behavior Analytics (Análisis de Comportamiento de Usuarios y Entidades) o sus siglas en inglés (UEBA) y el aporte importante que estas herramientas tienen para controlar el problema de fuga o robo de información.

Problema de investigación

La información de una empresa es un recurso muy importante que permite obtener varios beneficios como: prestigio, crecimiento del negocio y credibilidad ante posibles clientes. Cuando se produce una fuga de información y esta cae en manos equivocadas, las consecuencias pueden ser muy críticas tales como pérdidas económicas, mala reputación y pueden provocar el cierre de la empresa.

De ahí que es importante establecer una estrategia que permita mantener la información dentro de un entorno seguro. Dentro de estas estrategias está el uso de herramientas tecnológicas como las que se plantean en este documento y usan como concepto la tecnología UEBA, que permiten analizar el comportamiento de la gente que está conectada a una red organizacional y los equipos o entidades usados para su trabajo diario. Se denomina «gente» a un empleado o a usuarios externos a quienes se le ha otorgado el acceso a algún segmento de la red de la organización.

¿Basado en el uso de herramientas UEBA, se puede establecer una estrategia que permita controlar la fuga de información?

Objetivo general

Desarrollar una estrategia que permita el control específico de los usuarios que acceden a la información de la empresa usando la tecnología UEBA.

Objetivos específicos

Identificar mediante un análisis de vulnerabilidades, cuáles son los mecanismos que provocan la fuga de información con el propósito de minimizar esta amenaza.

Evidenciar los efectos o el impacto que puede causar la fuga de la información mediante la matriz de riesgos de tecnología de la empresa

Especificar las acciones previamente implementadas por la organización que permitan controlar la fuga de información mediante la revisión de la política de seguridad

Validar con un experto en seguridad informática, el diseño de la estrategia que permite controlar la fuga de información de la empresa.

Vinculación con la sociedad y beneficiarios directos:

El presente artículo está dirigido al personal de seguridad informática de empresas relacionadas con el área de construcción, quienes son responsables de definir políticas que permitan proteger la información de estas. Además, proponer una estrategia que permita implementar aplicaciones que utilicen la metodología UEBA, con el fin de identificar, generar acciones e implementar esta estrategia, mitigando el problema de fuga de la información.

Tomando como base el Objetivo de Desarrollo Sostenible de las Naciones Unidas número nueve que menciona «Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación», con el desarrollo de este documento se pretende realizar un aporte innovador a la forma de controlar y proteger la información a través de herramientas basadas en UEBA, lo cual permitirá mitigar el riesgo de fuga de ésta.

CAPÍTULO I: DESCRIPCIÓN DEL ARTÍCULO PROFESIONAL

La información en cualquier empresa es considerada como el bien más importante que tiene esta, siendo considerada como el activo principal, sin ésta las organizaciones no podrían efectuar sus operaciones de forma correcta y eficiente, incluso es más importante que los activos físicos. El objetivo principal es proteger la información conociendo las actividades que realizan las personas y evidenciando a los responsables de su uso. (Najar,Vacca, 2019)

1.1. Contextualización general del estado del arte

La acción de proteger la información implica tener en cuenta tres propiedades principales que son: **confidencialidad, integridad y disponibilidad.** El proceso de fuga de información se refiere a la ausencia de la confidencialidad, esto puede provocar que dicha información que debería ser solo conocida por un grupo específico de personas dentro de una empresa, sea visible o pueda ser accesible para personas que no hacerlo. (Revista UNIR, 2020)

Este documento plantea la necesidad de reconocer el origen y las causas principales que permiten la fuga de información, el impacto y consecuencias que se generan cuando existe un incidente de este tipo. La mayoría de las causas están asociadas al ámbito organizativo y por otro lado al ámbito técnico. Cualquiera que sea la causa implica que no existen medidas de seguridad, procedimientos o herramientas que permitan el control.

El objetivo de este documento es poder implementar una estrategia que implique el uso de una herramienta con tecnología UEBA la cual permita detectar el comportamiento del usuario, como el inicio de sesión en horas inusuales, los fallos excesivos de inicio de sesión y las eliminaciones de archivos de un servidor que generalmente no es utilizado por un usuario en particular.

Se ha realizado una investigación específicamente en el ámbito de la seguridad informática, y se ha detectado que existen muchos proveedores de aplicaciones UEBA. Hay una clasificación para estas aplicaciones diferenciadas por sí, que ayudan con el monitoreo de aplicaciones de software, la forma en que éstas obtienen los datos; o el método de entrega de los datos (On premise o en la nube). Según una guía de mercado generada por Gartner (2020), «El crecimiento de aplicaciones UEBA creció exponencialmente en 2020; los proveedores de estas soluciones aumentaron su cartera de clientes». El informe también permitió proyectar además que: «En los próximos años (3 aproximadamente), las principales plataformas UEBA serán las aplicaciones preferidas relacionadas con aspectos de seguridad. En algunos casos será mucho más fácil descubrir más eventos que otros sistemas de seguridad utilizados hasta hoy»

Investigaciones previas realizadas

Para poder realizar una mitigación en el problema de fuga de información se deben evaluar y comparar las diferentes herramientas que puedan ayudar a la aplicación de la estrategia que es razón de este documento. Los métodos formales incluyen software y elementos técnicos, como el hardware. La protección basada en software se puede aplicar a través de aplicaciones independientes o mediante soluciones de sistema como SIEM, SOAR y UEBA.

Hoy en día, las organizaciones utilizan estos sistemas a gran escala. Se debe considerar las definiciones de estas tres soluciones populares y los beneficios que cada una tiene para ofrecer.

A continuación, según Waitt (2019), se hace una breve descripción de las tres tecnologías:

SIEM (Security Information and Event Management**)**

Los equipos de TI usan soluciones SIEM para ayudar a protegerse contra las amenazas de seguridad, investigar y responder a las infracciones, controlar la pérdida de datos entre otras acciones. Las soluciones SIEM combinan el (SEM) que es la gestión de eventos de seguridad y el SIM que se refiere a la gestión de información de seguridad: Las soluciones SIEM brindan a las organizaciones visibilidad y control en tiempo real sobre lo que ocurre en la red.

SOAR (Orquestación, Automatización y Respuesta de Seguridad)

Se define como un conjunto de programas de software que permiten recopilar datos sobre amenazas de seguridad. A continuación, se detalla cada componente.

- Orquestación de seguridad: facilita la comunicación entre diferentes soluciones de seguridad de diferentes proveedores. Al modificar los datos de seguridad de formatos propietarios a formatos comunes que son más fáciles de almacenar, ayudan a agilizar la gestión de la información.

- Automatización de la seguridad: utiliza conjuntos de libros de jugadas conocidos para tomar medidas. Un analista no necesita intervenir manualmente. Al crear reglas para los tipos de alertas más recurrentes, por ejemplo, los equipos de operaciones de seguridad pueden dedicar menos tiempo a investigar falsos positivos repetitivos.

- Respuesta de seguridad: se ocupa de los problemas de seguridad confirmados. En entornos tradicionales, los analistas investigan y reaccionan a los incidentes manualmente. La automatización quita presión a los analistas. Acciones como deshabilitar el acceso a cuentas comprometidas se pueden realizar sin intervención humana. De este modo, los analistas pueden dedicar tiempo a atender cuestiones más apremiantes.

UEBA (User and Entity Behavior Analytics)

UEBA utiliza algoritmos, aprendizaje automático y análisis estadísticos para identificar las desviaciones de los patrones regulares e indica cuál de estas anomalías es una amenaza real. También puede usar UEBA para agregar los datos que tiene en registros e informes y para estudiar la información de flujo, archivo y paquete.

En UEBA, estudia todas las entidades (o puntos finales, como servidores, aplicaciones) y usuarios de su sistema, por lo que no supervisa eventos o dispositivos de seguridad. De esta manera, UEBA se adapta a las amenazas internas, como los empleados que se han visto comprometidos o se han vuelto deshonestos. UEBA también se dirige a las personas que ya han penetrado en su sistema.

Fuga de información

La fuga de información o filtración de datos supone un grave problema para muchas empresas a nivel mundial. Muchas empresas grandes y establecidas tienen dificultades para garantizar que los datos financieros, personales y técnicos se mantengan seguros. La fuga de información implica la exposición de información que facilita los ataques a las aplicaciones y los datos que estas manejan donde pueden estar importantes detalles de la organización. (Puente, 2019)

Fuga de información lógica

Según Kelsey (2002) se conoce como «salida de información no controlada cuyo destino conlleva a que ésta sea usada por personas equivocadas, esto provoca una pérdida de control de sus propietarios. Se considera como fuga de información cuando un software o elemento informático posee agujeros de seguridad lo que provoca que se encuentre afectada su integridad y permitiendo que atacantes de la red tanto interna como externa accedan a esos datos»

Otra forma que ayuda a la salida de información es el uso de impresoras y copiadoras, en donde un alto porcentaje de los empleados pueden tener libre acceso y provoca que un gran número de documentos que contienen información conocida como restringida como: clientes, ubicaciones, medios de contacto, entre otros, estén disponibles para cualquier persona, lo cual evidencia que no se lleva un proceso de borrado o destrucción adecuado de la información impresa y no se apega o se desconoce las políticas de seguridad física de la empresa en cuanto al manejo de desechos como el papel utilizado en las oficinas. Un alto porcentaje de la fuga de información es expuesta por el uso de: correos electrónicos, memorias o discos USB, por conexiones a una red inalámbrica, portales de alojamiento de archivos, nubes públicas, discos externos, o internet entre otros, lo cual no es adecuadamente controlado ya que lo que se logra bloquear por servidores o antivirus son los puertos USB y las unidades ópticas (CD, DVD). De acuerdo con el Reporte de Ciberseguridad de Cisco (2021) cuyo análisis se publica a nivel mundial, las principales conductas que provocan la fuga de información incluyen:

- **Aplicaciones no autorizadas**: los profesionales de TI (70%) explican que el uso de programas no autorizados o sin licencia es un factor clave para generar incidentes de pérdida de información en las empresas.
- **Uso inadecuado de equipos de la empresa**: los empleados comparten hasta en un 44% sus equipos de trabajo con otras personas sin la adecuada supervisión.
- **Acceso físico a zonas de la red**: los profesionales de TI (39%) afirman que el acceso no autorizado de un empleado a zonas de la red (como los racks de comunicaciones) puede generar un incidente.
- **Trabajo remoto**: un 46% de trabajadores suelen transferir información entre sus equipos de la empresa y sus equipos personales para trabajar desde el hogar.
- **Contraseñas comprometidas**: un gran porcentaje (18%) de los trabajadores comparten contraseñas con sus colegas o no cambian frecuentemente las mismas.

Clasificación de la información

Cada empresa tiene la potestad de clasificar la información que genera dependiendo del contenido y del destino de esta. De acuerdo con esa clasificación la empresa determina quién tiene acceso y de qué forma (permisos o autorizaciones) puede usar la misma para el desarrollo de su trabajo. La información generalmente está clasificada en base a su criticidad o nivel de visibilidad. Es responsabilidad del usuario que genera la información (Propietario) el identificar y clasificar según los siguientes tipos como se muestra a continuación

Tabla 1

Clasificación de la información

Tipo de Información	***Descripción***
Pública	Es la información que puede ser visible o divulgada por los empleados de la empresa, clientes o proveedores, sin el riesgo de que esta pueda afectar de manera alguna a la empresa
Sensible o de Uso Interno	Es sólo para uso interno, exclusivo de los trabajadores de la empresa, para el trabajo diario en las actividades de la organización. La visualización o divulgación de esta dentro de la empresa es permitida. Esta información debe mantenerse dentro de la compañía, ya que su divulgación externa podría generar impacto a la privacidad del personal, al negocio o a la imagen de la empresa.
Restringida	Información por su naturaleza de uso exclusivo de la empresa, puede ser accedida y visualizada expresamente por los empleados autorizados. La divulgación o visualización externa de la misma podría evidenciar la privacidad de los empleados, reducir la ventaja con sus competidores o causar un daño importante al negocio o al prestigio de la empresa.
Confidencial	Esta información es considerada muy sensible e importante, únicamente para uso interno, y con acceso a específico. La divulgación o visualización externa de la misma podría genera un problema serio ya que esta información evidencia datos claves de la empresa.

Nota: Autoría propia, basado en ISO 27001

Objetivos de la seguridad de la información

Según un artículo publicado por DocuSign (2021) dice: «Por el vertiginoso aparecimiento de los tipos de ataques y delitos cibernéticos, el resguardo de la información se ha convertido en el principal objetivo de las organizaciones. Sin embargo, es necesario conocer los pilares que soportan el uso de la información con el fin de incrementar la seguridad de esta. Estos pilares son: Confidencialidad, Integridad y Disponibilidad

Figura 1

Objetivos seguridad de la información

Nota: Autoría propia, basado en estudio de DocuSign

Tabla 2

Objetivos de la seguridad de la información

Objetivo	***Descripción***
Disponibilidad	Tiene relación con la accesibilidad que se tiene a los datos y a los sistemas corporativos
Integridad	Se refiere a la veracidad de la información y que se mantenga de esa forma no sea modificada o adulterada por personas sin autorización.
Confidencialidad	Establece las acciones con el objetivo de asegurar que los datos almacenados sean utilizados por personas autorizadas

Nota: Autoría propia, basado en estudio de DocuSign

1.2. Proceso investigativo metodológico

En esta investigación se utilizó el método bibliográfico comparativo, se procede con la lectura de material relacionado con User and Entity Behavior Analytics, artículos de investigación, tesis, implementaciones en otras organizaciones, determinando como las herramientas basadas en esta tecnología pueden ser parte de la estrategia para evitar el problema de fuga de información.

Luego de este análisis se define como una herramienta UEBA puede formar parte de la estrategia a definir en este documento y cómo ayudaría al personal de tecnología a detectar posibles intentos de robo o fuga de información de las organizaciones. Como parte de la estrategia a implementar se hace necesario definir los actores y factores que causan el problema de fuga de información

Aspectos técnicos

Hace relación a la complejidad para administrar y gestionar cantidades grandes de datos que procesan las empresas. En ese entorno hay que controlar de manera adecuada el acceso que los usuarios tienen a archivos que estén relacionados con su trabajo y la cual puede ser enviada fuera de la empresa. Una de las principales debilidades es el uso del malware el cual permite el acceso a los equipos y que afectan de manera directa. Otra forma de ataque es el efecto de capturar las contraseñas de los usuarios con las cuales se puede acceder a la información. Adicional a estos aspectos puede surgir una fuga de información generada por errores técnico que provocan que esta información quede expuesta y sin control. (Mackay, 2021)

Para contrarrestar los problemas relacionados con el aspecto técnico han aparecido herramientas como: Information Leak Detection and Prevention (IDLP), , Content Monitoring and Filtering (CMF), Information Leak Prevention (ILP), Information Protection and Control (IPC), Data Loss Prevention (DLP). Estos mecanismos ayudan a monitorear y controlar la información que circula en una infraestructura y bloquean el acceso o conexión de dispositivos no confiables.

Aspectos humanos

Lo normal es que una persona no tenga la necesidad de robar información de manera intencional. Sin embargo, este comportamiento puede ser causado por empleados inconformes con la empresa o que se sienta perjudicado por la misma. Así mismo, pueden existir empleados que realicen espionaje interno y compartan la información de manera intencional con la competencia.

De todos modos, la fuga de información no puede darse sólo por una mala intención del usuario, sino que en muchos casos el ataque externo intenta conseguir información engañando al usuario. Un ejemplo es un malware que viaja en una memoria USB y ahí se ve la importancia de tener instalado algún sistema que permita anticiparse al ataque.

Factores comunes de fuga de información

Debido al avance vertiginoso de la tecnología existen muchas maneras en que la información de una empresa puede filtrarse a terceras personas no autorizadas. La fuga de información puede ser involuntaria, causada por problemas de seguridad dentro de la empresa o deliberada, causada por el factor humano.

Tabla 3

Factores comunes de fuga de información

Riesgo	***Efecto***	***Controles***
Conexión de dispositivos móviles personales a la red de la empresa.	Acceso a información no autorizada	Restringir la conexión de dispositivos personales a la red de la empresa
Conexión de dispositivos de almacenamiento externo	Copia de información de la empresa	Bloquear el uso de puertos USB o CD/DVD en los equipos de la empresa
Uso de correo electrónico	Envío o salida de información de la empresa usando este medio	Controlar el contenido del correo incluyendo anexos

Uso de redes inalámbricas no confiables	Acceso a la información almacenada en los computadores de la empresa	Evitar el uso de redes desconocidas
Uso de aplicaciones en la nube	Acceso no autorizado a información en la nube	Gestionar permisos de usuarios y carpetas
Uso de redes sociales	Filtración de información personal y de la empresa	Bloquear el acceso a redes sociales
Malware, virus	Infección o pérdida de información por ataques de este tipo	Implementar antivirus y otras herramientas corporativas en los equipos de la empresa
Credenciales inseguras	Acceso por personal no autorizado	Implementar el uso de contraseñas complejas

Nota: Autoría propia, basado en informe de CISCO (2018)

Información en empresas de construcción

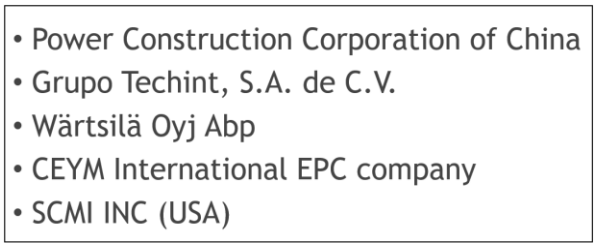
Las empresas de construcción en el Ecuador en general se basan en un modelo de Ingeniería, Procura y Construcción, que especifica que cuando se realiza un contrato, la empresa contratista como tal se encargará del diseño de la Ingeniería, la adquisición o compra de los materiales, equipos e insumos necesarios para poder cumplir con el contratante y adicionalmente gestionan y ejecutan la construcción dentro del proyecto asignado.

Para iniciar una licitación es muy importante partir de un presupuesto que incluye recursos económicos, humanos y tecnológicos. Esta información es la base para poder ganar un proyecto.

Basados en este antecedente se puede determinar que esta información es vital para poder ser contratado por la empresa que tiene un proyecto. Si esta información llega a manos de una empresa de la competencia de forma voluntaria o involuntaria (Fuga de información), se corre el riesgo de perder el proyecto ya que la empresa que logra conseguir esta tiene una ventaja competitiva pues puede reducir los tiempos de ejecución y bajar sus costos, con el fin de ganar la licitación.

Figura 2

Principales empresas EPC en Ecuador



Nota: Autoría propia, basado en estudio de Mordor Intelligence

Acciones previamente implementadas

El estado actual de la seguridad implementada en la empresa SCMI INC USA incluyen varios mecanismos que permiten mitigar el proceso de fuga de información como son:

- Redes inalámbricas restringidas
- Antivirus corporativo
- Firewall perimetral
- Política de credenciales con complejidad
- Autenticación de doble factor
- Política de permisos de acceso la información
- Política de utilización de computadores personales
- Bloqueo de sitios de almacenamiento masivo (Dropbox, OneDrive, etc)

1.3. Análisis de resultados

Aparte de la forma en que se usan las herramientas de seguridad como UEBA, es necesario involucrar uno de los elementos más críticos para reforzar su seguridad que es el empleado y su conocimiento sobre las prácticas de ciberseguridad recomendadas.

- **Entrenar al personal:** Asegurar que los empleados de la organización tienen conocimientos sobre los ataques informáticos y sus consecuencias.
- **Considerar las amenazas internas:** Configurar la herramienta UEBA de forma que pueda detectar amenazas internas
- **Bloquear el acceso:** Solamente el personal de la empresa debe tener acceso a los datos
- **Controlar los privilegios:** Configurar la herramienta UEBA para alertar sobre cambios en los permisos de los usuarios sobre la información corporativa

- **Usar herramientas adicionales:** Complementar a UEBA con otras herramientas tradicionales de monitoreo de su infraestructura.

Uso de herramientas UEBA para proteger la información

Proporcionan análisis sobre el comportamiento del usuario y su accionar sobre sus estaciones de trabajo, redes y aplicaciones. Los resultados de este análisis generan información precisa y ayuda en la detección de amenazas manera más eficaz.

Tabla 4

Ventajas y Desventajas de herramientas UEBA

Ventajas	***Desventajas***
Permite detectar automáticamente una amplia gama de ciberataques. Estos incluyen amenazas internas, cuentas comprometidas, ataques de fuerza bruta, la creación de nuevos usuarios y violaciones de datos.	Costo inicial. Mientras que para las empresas más grandes una inversión en UEBA se amortizará rápidamente, es posible que las empresas más pequeñas no necesiten una solución de monitorización tan compleja.
Los sistemas automatizados pueden reducir drásticamente la cantidad de analistas de seguridad que se necesita emplear.	Los datos generados por UEBA son más complejos que los generados por sistemas UBA más básicos. Esto puede dificultar la comprensión de los analistas de seguridad.
Reducción significativa de tu presupuesto de ciberseguridad	UEBA no sustituye a otros sistemas de ciberseguridad. Permitirá detectar un comportamiento inusual, pero no realiza un proceso de bloqueo a los intrusos.

Nota: Autoría propia, basado en estudio de DocuSign

Comparativa de herramientas y precios de implementación

Existe un número importante de empresas de software que ofrecen soluciones UEBA. Dependiendo de cada una se pueden encontrar soluciones con instalaciones On-Premises o en la nube. Difiere su costo de acuerdo con el método de licenciamiento. En la tabla siguiente se muestran varias opciones de soluciones UEBA.

Tabla 5

Comparativa de Herramientas UEBA

Solución	***Empresa***	***Funcionalidad***	***Instalación***	***Escalable***	***Precio***
Aruba	Hewlett Packard	Solución que utiliza el aprendizaje automático para detectar, priorizar, investigar y responder a ataques internos sigilosos.	Versiones de dispositivos y solo software	Ilimitada	Basado en el número de entidades monitoreadas
Dtex	Dtex Systems	Proporciona visibilidad de toda la actividad dmel usuario sin importar dónde se lleva a cabo, dentro o fuera de la red corporativa	On-Premises software	Ilimitada	$2 por usuario/mes. Cotizaciones bajo pedido.
Exabeam	Exabeam INC	Ayuda a los equipos de seguridad a superar las probabilidades al agregar inteligencia a sus herramientas de seguridad existentes, incluidos SIEM,	Dispositivo físico o máquina virtual en la nube	Ilimitada	Cotizaciones disponibles bajo petición
Forcepoint Inisder Threat	Forcepoint	Solución que permite generar una alerta temprana sobre una amenaza interna y permite evitar el filtrado de sus datos regulados	On-premises software	Ilimitada	Cotizaciones disponibles bajo petición
FortiInsight	Fortinet	Protege a las organizaciones de las amenazas internas al monitorear continuamente a los usuarios y puntos finales con capacidades de detección y respuesta automatizadas	Solucion Cloud	Ilimitada	Con licencia basada en el número de puntos finales protegidos

Fortscale	RSA Security	Análisis de comportamiento de usuarios, específicamente en análisis diseñados para contrarrestar amenazas internas	Software local (solo Linux)	Ilimitada	Cotizaciones disponibles bajo petición
Gurucul Risk Analytics	Amazon Web Services	Ofrece tres tipos diferentes de análisis de seguridad: UEBA, análisis de identidad y análisis de seguridad en la nube	Dispositivo, máquina virtual, nube	Ilimitada	Cotizaciones disponibles bajo petición
Interset	CyberRes	Análisis avanzados, inteligencia artificial y experiencia en ciencia de datos a sus soluciones de seguridad	Dispositivo físico o máquina virtual para la nube	Ilimitada	Cotizaciones disponibles bajo petición
LogRhythm UEBA	LogRhythm	Implementa el aprendizaje automático para detectar anomalías basadas en el usuario y sus acciones	Dispositivo físico o máquina virtual para la nube	Ilimitada	Comienza en $115/entidad por año
Microsoft Sentinel	Microsoft	Ayuda a identificar actividades anómalas y ayuda a determinar si un recurso se ha puesto en peligro.	Solo Cloud	Ilimitada	Inicia en $80/ usuario por año
Palo Alto Cortex XDR	Palo Alto	Descubre amenazas mediante el análisis de comportamiento, acelera las investigaciones con la automatización y detiene los ataques antes de que se produzcan daños	Solo Cloud	Ilimitada	Cotizaciones disponibles bajo petición
Splunk User Behavior Analytics	Splunkbase	Es una solución impulsada por el aprendizaje automático que ayuda a las organizaciones a encontrar amenazas ocultas y comportamientos anómalos entre usuarios, dispositivos y aplicaciones	On-premises software or alojado como AWS service	Ilimitada	Cotizaciones disponibles bajo petición

Nota: Autoría propia, basado en análisis de Project-management.com

CAPÍTULO II: ARTÍCULO PROFESIONAL

1.1. Resumen

En la actualidad la información en cualquier empresa es considerada como el bien más importante que tiene esta, siendo considerada como el activo principal, sin ésta las organizaciones no podrían efectuar sus operaciones de forma correcta y eficiente, incluso es más importante que los activos físicos. El objetivo principal es proteger la información conociendo los responsables y los escenarios en los que trabajan. Los datos adecuadamente asegurados ayudan a las organizaciones a volver a crecer inclusivo si no existieran instalaciones físicas. En el presente documento se desea plantear una estrategia que permita evitar la fuga o robo de información usando como base el uso de herramientas User and Entity Behavior Analytics (UEBA).

Palabras clave: fuga, UEBA, comportamiento, seguridad

1.2. Abstract

At present, information in any company is considered the most important asset that it has, being considered the main asset, without it, organizations could not carry out their operations correctly and efficiently, it is even more important than physical assets. The main objective is to protect the information by knowing who is responsible and the scenarios in which they work. Properly secured data helps organizations grow back inclusive if physical facilities did not exist. In this document we want to propose a strategy that allows avoiding the leakage or theft of information using as a base the use of User and Entity Behavior Analytics (UEBA) tools.

a. Keywords: leak, UEBA, behavior, security

1.3. Introducción

La información en cualquier empresa es considerada como el bien más importante que tiene esta, siendo considerada como el activo principal, sin ésta las organizaciones no podrían efectuar sus operaciones de forma correcta y eficiente, incluso es más importante que los activos físicos. El objetivo principal es proteger la información conociendo las actividades que realizan las personas y evidenciando a los responsables de su uso. (Najar,Vacca, 2019)

Con el transcurrir del tiempo y el vertiginoso avance tecnológico, las amenazas también han evolucionado y se han identificado dos orígenes principales de estas: el origen interno que tiene que ver con los incidentes de seguridad provocados por personal de las

propias organizaciones y el de origen externo que es provocado por ataques cuyo objetivo es conseguir rédito económico o dañar la imagen de la empresa (Yulima Hernandez, 2022)

Acorde a InsightExpress (2018) a pesar de que la organización haya elaborado políticas o procedimientos en cuanto a la seguridad, existen conductas arriesgadas que ponen en peligro la información empresarial como la personal. Dichas conductas podrían ser:

- Uso de software no autorizado
- Uso de computadores de la organización para trabajos personales
- Permitir el acceder a la red de la empresa a gente no autorizada
- Uso no adecuado de claves o compartir estas con otras personas

Este documento plantea la definición una estrategia que permita identificar y posteriormente mitigar el riesgo asociado con la fuga de datos. Además, se tiene como objetivo el análisis de las herramientas User and Entity Behavior Analytics (Análisis de Comportamiento de Usuarios y Entidades) o sus siglas en inglés (UEBA) y el aporte importante que estas herramientas tienen para controlar el problema de fuga o robo de información.

1.4. Metodología

En esta investigación se utilizó el método bibliográfico comparativo, se procede con la lectura de material relacionado con User and Entity Behavior Analytics, artículos de investigación, tesis, implementaciones en otras organizaciones, determinando como las herramientas basadas en esta tecnología pueden ser parte de la estrategia para evitar el problema de fuga de información.

Luego de este análisis se define como una herramienta UEBA puede formar parte de la estrategia a definir en este documento y cómo ayudaría al personal de tecnología a detectar posibles intentos de robo o fuga de información de las organizaciones. Como parte de la estrategia a implementar se hace necesario definir los actores y factores que causan el problema de fuga de información

Aspectos técnicos

Hace relación a la complejidad para administrar y gestionar cantidades grandes de datos que procesan las empresas. En ese entorno hay que controlar de manera adecuada el acceso que los usuarios tienen a archivos que estén relacionados con su trabajo y la cual

puede ser enviada fuera de la empresa. Una de las principales debilidades es el uso del malware el cual permite el acceso a los equipos y que afectan de manera directa. Otra forma de ataque es el efecto de capturar las contraseñas de los usuarios con las cuales se puede acceder a la información. Adicional a estos aspectos puede surgir una fuga de información generada por errores técnico que provocan que esta información quede expuesta y sin control. (Mackay, 2021)

Para contrarrestar los problemas relacionados con el aspecto técnico han aparecido herramientas como: Information Leak Detection and Prevention (IDLP), , Content Monitoring and Filtering (CMF), Information Leak Prevention (ILP), Information Protection and Control (IPC), Data Loss Prevention (DLP). Estos mecanismos ayudan a monitorear y controlar la información que circula en una infraestructura y bloquean el acceso o conexión de dispositivos no confiables.

Aspectos humanos

Lo normal es que una persona no tenga la necesidad de robar información de manera intencional. Sin embargo, este comportamiento puede ser causado por empleados inconformes con la empresa o que se sienta perjudicado por la misma. Así mismo, pueden existir empleados que realicen espionaje interno y compartan la información de manera intencional con la competencia.

De todos modos, la fuga de información no puede darse sólo por una mala intención del usuario, sino que en muchos casos el ataque externo intenta conseguir información engañando al usuario. Un ejemplo es un malware que viaja en una memoria USB y ahí se ve la importancia de tener instalado algún sistema que permita anticiparse al ataque.

Factores comunes de fuga de información

Debido al avance vertiginoso de la tecnología existen muchas maneras en que la información de una empresa puede filtrarse a terceras personas no autorizadas. La fuga de información puede ser involuntaria, causada por problemas de seguridad dentro de la empresa o deliberada, causada por el factor humano.

Tabla 6

Factores comunes de fuga de información

Riesgo	Efecto	Controles
Conexión de dispositivos móviles personales a la red de la empresa.	Acceso a información no autorizada	Restringir la conexión de dispositivos personales a la red de la empresa

Conexión de dispositivos de almacenamiento externo	Copia de información de la empresa	Bloquear el uso de puertos USB o CD/DVD en los equipos de la empresa
Uso de correo electrónico	Envío o salida de información de la empresa usando este medio	Controlar el contenido del correo incluyendo anexos
Uso de redes inalámbricas no confiables	Acceso a la información almacenada en los computadores de la empresa	Evitar el uso de redes desconocidas
Uso de aplicaciones en la nube	Acceso no autorizado a información en la nube	Gestionar permisos de usuarios y carpetas
Uso de redes sociales	Filtración de información personal y de la empresa	Bloquear el acceso a redes sociales
Malware, virus	Infección o pérdida de información por ataques de este tipo	Implementar antivirus y otras herramientas corporativas en los equipos de la empresa
Credenciales inseguras	Acceso por personal no autorizado	Implementar el uso de contraseñas complejas

Nota: Autoría propia, basado en informe de CISCO (2018)

Investigaciones previas realizadas

Para poder realizar una mitigación en el problema de fuga de información se deben evaluar y comparar las diferentes herramientas que puedan ayudar a la aplicación de la estrategia que es razón de este documento. Los métodos formales incluyen software y elementos técnicos, como el hardware. La protección basada en software se puede aplicar a través de aplicaciones independientes o mediante soluciones de sistema como SIEM, SOAR y UEBA.

Hoy en día, las organizaciones utilizan estos sistemas a gran escala. Consideremos las definiciones de estas tres soluciones populares y los beneficios que cada una tiene para ofrecer.

A continuación, según Waitt (2019), se hace una breve descripción de las tres tecnologías:

SIEM (Security Information and Event Management**)**

Los equipos de TI usan soluciones SIEM para ayudar a protegerse contra las amenazas de seguridad, investigar y responder a las infracciones, controlar la pérdida de

datos entre otras acciones. Las soluciones SIEM combinan el (SEM) que es la gestión de eventos de seguridad y el SIM que se refiere a la gestión de información de seguridad:

Las soluciones SIEM brindan a las organizaciones visibilidad y control en tiempo real sobre lo que ocurre en la red.

SOAR (Orquestación, Automatización y Respuesta de Seguridad)

Se define como un conjunto de programas de software que permiten recopilar datos sobre amenazas de seguridad. A continuación, se detalla cada componente.

- Orquestación de seguridad: facilita la comunicación entre diferentes soluciones de seguridad de diferentes proveedores. Al modificar los datos de seguridad de formatos propietarios a formatos comunes que son más fáciles de almacenar, ayudan a agilizar la gestión de la información.

- Automatización de la seguridad: utiliza conjuntos de libros de jugadas conocidos para tomar medidas. Un analista no necesita intervenir manualmente. Al crear reglas para los tipos de alertas más recurrentes, por ejemplo, los equipos de operaciones de seguridad pueden dedicar menos tiempo a investigar falsos positivos repetitivos.

- Respuesta de seguridad: se ocupa de los problemas de seguridad confirmados. En entornos tradicionales, los analistas investigan y reaccionan a los incidentes manualmente. La automatización quita presión a los analistas. Acciones como deshabilitar el acceso a cuentas comprometidas se pueden realizar sin intervención humana. De este modo, los analistas pueden dedicar tiempo a atender cuestiones más apremiantes.

UEBA (User and Entity Behavior Analytics)

UEBA utiliza algoritmos, aprendizaje automático y análisis estadísticos para identificar las desviaciones de los patrones regulares e indica cuál de estas anomalías es una amenaza real. También puede usar UEBA para agregar los datos que tiene en registros e informes y para estudiar la información de flujo, archivo y paquete.

En UEBA, estudia todas las entidades (o puntos finales, como servidores, aplicaciones) y usuarios de su sistema, por lo que no supervisa eventos o dispositivos de

seguridad. De esta manera, UEBA se adapta a las amenazas internas, como los empleados que se han visto comprometidos o se han vuelto deshonestos. UEBA también se dirige a las personas que ya han penetrado en su sistema.

1.5. Resultados y Discusión

Resultados

Independientemente de la herramienta UEBA que se haya seleccionado de acuerdo con las funcionalidades técnicas y el presupuesto, se plantea el modelo para la estrategia de implementación de la solución.

Primer paso: Recopilación de información

Lo primero en esta etapa es permitir a la herramienta el coleccionar datos sobre el comportamiento del usuario y su interacción diaria sobre las entidades (aplicaciones, dispositivos, páginas web) usadas con más frecuencia. La herramienta podría recopilar la siguiente información sobre la actividad de los usuarios:

- Horas de inicio y cierre de sesión en la red
- Requerimientos de acceso a servicios sensibles
- Páginas web visitadas
- Aplicaciones usadas
- Dispositivos conectados a su estación de trabajo

Segundo paso: Detección de amenazas

Luego de que la solución de análisis ha recopilado la información del comportamiento del usuario, UEBA le permite detectar amenazas internas, además detecta acciones sospechosas y establece patrones para las diferentes categorías de usuarios. Dentro de la estrategia de amenazas internas UEBA le ayuda, por ejemplo:

- Detectar una amenaza basada en la acción de cada usuario en tiempo real. Por ejemplo, un empleado tiene asociado dentro de la herramienta su horario de trabajo. Dentro de ese período de tiempo es normal efectuar eventos de inicio y cierre de sesión. Si este mismo usuario intenta iniciar sesión fuera de ese horario, la herramienta puede alertar al supervisor de la herramienta o bloquear ese intento.
- Priorizar las alertas. UEBA puede crear una lista de acciones sospechosas y categorizar éstas de acuerdo con su nivel de criticidad o impacto.

- Mejorar la eficiencia al detectar ataques maliciosos. Esto permite determinar las acciones a tomar para minimizar el efecto del ataque o evitarlo a futuro.

Tercer paso: Creación de perfiles de comportamiento

Cuando se trata de amenazas internas, un perfil de comportamiento le permite crear una línea base de cómo el usuario interactúa dentro de la red. Esta línea ayuda a UEBA en la detección de acciones anormales de un usuario. Esta funcionalidad es valiosa ya que permite anticipar incidentes.

Cuarto paso: Generar alerta temprana

La solución UEBA puede detectar anomalías en el comportamiento de un empleado que indica una acción maliciosa. La alerta temprana significa que se puede detectar un incidente antes de que suceda. Como ejemplo, la herramienta puede alertar que un usuario trabaja fuera de horario, accediendo a información confidencial a la cual el usuario no requería anteriormente, o conectar un dispositivo de almacenamiento externo que nunca ha usado.

Quinto paso: Prevenir amenazas internas

La solución UEBA puede crear una escala de puntajes de riesgo, mucho antes de que se cometa un ataque No es necesaria la intervención de un encargado de seguridad pues esta escala se genera basada en:

- Perfil de comportamiento del usuario
- Patrones de ataques internos
- Privilegios del usuario sobre los datos o sistemas

Sexto paso: Actualizar perfiles con regularidad

Es probable que sea necesario reconstruir o actualizar la información de las actividades de los usuarios, ya que sus actividades sobre la red pueden cambiar de acuerdo con el puesto que ocupa el empleado. Si existe un ascenso o cambio de puesto el sistema UEBA deberá aprender nuevamente y generar un nuevo perfil para este usuario.

Discusión

El uso de las herramientas UEBA no se limita a grandes organizaciones con presupuestos onerosos en el área de TI. Muchas empresas pequeñas enfrentan amenazas a la seguridad de su información por lo que se puede adoptar soluciones de código abierto a nivel de SIEM, sin embargo, las herramientas UEBA al ser herramientas más especializadas el encontrar soluciones de código abierto es limitado.

Afortunadamente la mayoría de las soluciones de pago son escalables, es decir, pueden adaptarse al tamaño de la organización e ir creciendo de acuerdo con la demanda que requiera la misma.

CONCLUSIONES

Realizando una correcta clasificación de la información e implementando una herramienta UEBA, las empresas y los equipos de TI pueden detectar con facilidad un intento de fuga de información, además se podrán realizar las correcciones necesarias sobre las brechas de seguridad que permiten este comportamiento. En el caso de la empresa SCMI INC (USA) que es caso de estudio se realizó por una entidad externa una prueba de vulnerabilidades donde se evidencia que es necesario aplicar las recomendaciones de este para minimizar los riesgos de seguridad.

Es importante entender que la fuga de información genera impactos severos sobre la empresa que sufre un ataque, algunos de los efectos pueden ser: pérdidas financieras, daño de la imagen, problemas legales e incluso la interrupción de la actividad de la compañía. Para el caso de la empresa SCMI INC (USA), se ha desarrollado un plan

La empresa SCMI INC (USA) ha implementado varias acciones que permiten controlar de alguna manera el problema de fuga de información mediante la creación y difusión de una política interna denominada “Gestión de Seguridad”, sin embargo, es necesario modificar la misma con el fin de implementar una herramienta UEBA.

Se ha validado con un experto en seguridad informática, si la estrategia diseñada para la implementación de una herramienta UEBA dentro de la empresa está correctamente elaborada con el fin de mitigar el riesgo que es estudio de este documento.

RECOMENDACIONES

Para realizar una implementación adecuada de cualquier estrategia que permita controlar el problema de fuga de información es necesario concientizar tanto a los empleados, a los equipos de TI y a la dirección de la empresa sobre la importancia de la información corporativa, hacer conocer sobre los efectos de que esta se filtre o sea conocida por personas ajenas a la organización.

Se hace indispensable contar con una política de gestión de seguridades donde se establezca claramente la clasificación de la información de la empresa y los procedimientos de acceso a la misma. Adicionalmente cada empleado debería firmar un acuerdo de confidencialidad en el cual se comprometa a no divulgar la información de la compañía a terceros.

Luego de realizar todos los pasos previos se puede iniciar con la implementación de una herramienta basada en tecnología UEBA, la cual permita a futuro minimizar el riesgo de fuga de información.

BIBLIOGRAFÍA

Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020). *Ciberseguridad.* Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro.net/es/lc/uisrael/titulos/172144

Barría Huidobro, C. (2020). *Nuevos espacios de seguridad nacional: cómo proteger la información en el ciberespacio*. Editorial ebooks Patagonia - Ediciones UM. https://elibro.net/es/lc/uisrael/titulos/195463

Docusign, (2021). *¿Cuáles son los pilares de la seguridad de la información?* DocuSign https://www.docusign.mx/blog/seguridad-de-la-informacion

Hernandez, Y. (2022). *¿Qué es una amenaza en seguridad Informática y cómo prevenirla?* Dongee. https://www.dongee.com/tutoriales/que-es-una-amenaza-en-seguridad/

Mackay, J. (2021). *Riesgos De Ciberseguridad: ¿Factores Humanos O Fallos Humanos?* MetaBlog. https://www.metacompliance.com/es/blog/cyber-security-awareness/cyber-security-risk#:~:text=Los%20factores%20humanos%20son%20utilizados,ciberdelincuencia%20ser%C3%ADa%20mucho%20m%C3%A1s%20dif%C3%ADcil.

Najar Pacheco, José Custodio & Vacca -Visión Electrónica, Harold. (2017). *Exposición del activo más valioso de la organización, la "información".* ResearchGate. https://www.researchgate.net/publication/338569397_Exposicion_del_activo_mas_valioso_de_la_organizacion_la_informacion

Puente, L. (2019). *Fugas de información, un problema para las empresas.* SIMAD. https://www.si-mad.com/fugas-de-informacion-un-problema-para-las-empresas/

Ramos Mera, J. M. (2020). *Delitos contra la seguridad de los activos de los sistemas de información y comunicación en el Ecuador.* Corporación de Estudios y Publicaciones. https://elibro.net/es/lc/uisrael/titulos/171995

Rivioralta, J. (2021). *La información, un activo vital para tu empresa.* Incibe. https://www.incibe.es/protege-tu-empresa/blog/informacion-activo-vital-tu-empresa

Salitin, Manya & Zolait, Ali. (2018). *The role of User Entity Behavior Analytics to detect network attacks in real time*. ResearchGate. https://www.researchgate.net/publication/336259455_The_role_of_User_Entity_Behavior_Analytics_to_detect_network_attacks_in_real_time

UNIR (2020). *Principios de la seguridad informática: consejos para la mejora de la ciberseguridad.* Unir Revista. https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/

Waitt, T. (2019). *SIEM, UEBA, and SOAR – What´s the difference?* American Secutiry Today. https://americansecuritytoday.com/siem-ueba-and-soar-whats-the-difference/

ANEXOS

ANEXO 1

INFORME DE ANÁLISIS DE VULNERABILIDADES (TECNISEGUROS) USANDO SECURITYSCORECARD

ANEXO 2

MATRIZ DE RIESGOS DE TECNOLOGÍA SCMI INC (USA)

ANEXO 3

POLITICA DE GESTION DE SEGURIDAD

ANEXO 4

VALIDACIÓN DE LA ESTRATEGIA