Universidad de Buenos Aires.

Facultades de Ciencias Económicas, Ciencias Exactas Naturales e Ingeniería.

Carrera de Especialización en Seguridad Informática.

Trabajo Final.

Tema: “Proyecto de aplicación profesional”

Título: “Implementación profesional de un Proyecto de Seguridad Informática: relevamiento de controles y propuestas de mejoras”

Autora: Lic. Abigail Kauf

Tutor: Mg. Diego Escobar.

Año de presentación: 2018

Cohorte de la cursante: 2017

Contenido

Declaración Jurada del Origen de los Contenidos

Por medio del presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis o Trabajo Final de Especialización vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Abigail Kauf
DNI 34.646.428

Resumen

La seguridad Informática dentro de la organización ocupa un papel preponderante en los tiempos que corren. No solo el manejo de las nuevas tecnologías de la información y de la comunicación sino también el resguardo de los datos de la compañía. La administración de los perfiles y roles de los usuarios, así como la interacción entre estos últimos dos, implican un desafío constante de aprendizaje.

En línea con este desafío, el presente trabajo de aplicación profesional tiene por objetivo relevar controles con sus correspondientes periodicidades, técnicas, herramientas utilizadas y métodos de ejecución en el área de Seguridad Informática Operativa, dentro de la dirección de Seguridad Informática de la empresa “Identidad Privada”. El área de referencia es la encargada de llevar adelante controles preventivos y correctivos sobre la operatoria de la seguridad informática interna de la compañía.

El relevamiento de los controles implica una comprensión detallada de la tarea que se está controlando, así como la población involucrada y la causa de los desvíos que se registran. Se encontrará en este trabajo un estudio exhaustivo sobre la información que nutre a los controles, y los agentes implicados en la tarea controlada, con el fin de identificar claramente cuáles son los riesgos para una posterior propuesta de mitigación.

Se pretende, al finalizar el relevamiento del área, entender cuáles son los controles principales, con qué objetivos se realizan, cuáles son las herramientas involucradas y la metodología por la cual buscan proteger la información. Para poder llevar adelante este análisis considero necesario mencionar los que los marcos teóricos de referencias y buenas prácticas mencionan al respecto.

A posteriori, podría utilizarse este trabajo para realizar mediciones sobre los controles que permitan traducir la información que se desprende de ellos a gráfico y cifras. El objetivo de estos controles es poder tomar decisiones para la mejora en la implementación de los mismo u optimización de la tarea.

Introducción

El presente trabajo de aplicación profesional tiene por objetivo relevar la tarea diaria que realiza un analista de seguridad informática operativa perteneciente a una organización multinacional e industrial.

En los primeros capítulos, describo el marco conceptual vinculando teóricamente normas, procedimientos y buenas prácticas de seguridad de la información. El mismo sentará una base de conocimiento sólida sobre la cual me basaré para cotejar la realidad de los controles empresariales con lo sugerido por la teoría.

En una segunda parte, analizaré en detalle los controles citados. Considerando anotaciones y salvedades producto del ejercicio profesional tales como: que en algunos de ellos se detectó que no tenían el alcance que el área pretendía, que podían mejorarse agregando una instancia más de control o bien que podían ser automatizados en cierto grado permitiendo ser más eficientes en el uso de los recursos.

Por último, arribare a conclusiones sobre el trabajo realizado hasta el momento reflexionando sobre alternativas superadoras y proponiendo un camino de mejora de cara al futuro y evolución del área.

Considerando que la Seguridad Informática posee un nivel de madurez entre tres y cuatro, basado en el Modelo de Madurez de Capacidad del Instituto de Ingeniería de Software (SEI CMMI), en las diferentes áreas en las que están segregadas la dirección de seguridad informática, creemos que relevar los controles y lo relacionados a ellos permitirá a la organización gestionar eficazmente los recursos disponibles y maximizar sus beneficios.

Justificación del tema elegido

Debido a la labor que realizo a diario en el área de Seguridad Informática Operativa, dentro de la dirección de Seguridad informática de la empresa

"Identidad Privada", elijo desarrollar este proyecto ya que considero que aportará a mi labor cotidiana. A su vez, colaborará con el delineado de mi perfil profesional, el cual requiere conocimiento técnico con el objetivo de tener una óptica integral de las medidas de gestión a aplicar.

Aportes prácticos al campo temático

No se debe perder de vista que se persigue brindar soporte y acompañar la evolución de la compañía “Identidad Privada” desde una perspectiva operativa de seguridad de la información considerando los recursos disponibles. El proceso de entender los requerimientos, los objetos de control y las herramientas involucradas en los mismos permitirá elevar el grado de conocimiento haciendo más eficiente la labor.

Con la observación de los resultados se podrán adoptar medidas correctivas, hacer foco en aquellos procesos que destaquen como críticos persiguiendo su mejora, o bien asegurarse de que las tareas desarrolladas cumplan con su objetivo. También, dichos controles están diseñados para alertar a los responsables del monitoreo sobre cualquier excepción que no esté alineada a las políticas de seguridad diseñadas por la empresa.

Objetivos y alcance

Objetivo General

En el marco del presente trabajo se propone como objetivo principal desarrollar un proyecto de Seguridad Informática que involucra la descripción, evaluación y análisis de cinco controles ejecutados por la compañía de forma rutinaria.

Objetivos particulares

El presente trabajo final de especialización tiene como objetivos particulares:

1. Relevar controles pertenecientes al área de seguridad informática de "Identidad Privada".
2. Documentar un proyecto de seguridad informática referente al análisis, desarrollo y ejecución de los controles.
3. Identificar y proponer aspectos de mejoras en los controles.
4. Sentar las bases para el desarrollo particular de métricas sobre Seguridad de la Información basadas en los controles.

Alcance

Se aclara que no existen al día de la fecha mediciones desarrolladas y en vigencia sobre estos procesos. Se propone analizarlos exhaustivamente teniendo en cuenta todas las aplicaciones de soporte, automatizaciones y tareas implicadas en su ejecución, midiendo tiempos de respuesta, performances, satisfacción del cliente interno, recursos implicados y posibles mejoras.

El alcance del trabajo es meramente profesional y su impacto será evaluado por los coordinadores y gerente del área, pudiendo demostrar de forma fehaciente una satisfactoria implementación con mejoras tangibles.

Pretende también, sentar las bases para el desarrollo de métricas en áreas que hayan alcanzado al menos un nivel 3 de madurez, según el CMMI arriba ya citado, aspirando a aplicar las propuestas de este trabajo en pos de aproximarse a un nivel 4 de madurez.

1. CAPÍTULO I: Identificación del Marco Teórica de los Controles y Monitorios en Seguridad Informática.

Para una mejor conceptualización de los controles que describiremos debajo y un contexto teórico que sustente la práctica diaria del área operativa, como paso previo a ahondar en los controles tal y como los implementa "Identidad Privada" en su área de Seguridad Informática, daré un marco teórico de contexto basándome en el Informe COSO II, COBIT 5, la norma ISO/IRAM 9001, la ISO/IEC/IRAM 27001 y 27002.

Es interesante destacar de manera introductoria la definición de las actividades de control tal y como la hace la norma COSO II “son las acciones establecidas por políticas y procedimientos para ayudar asegurar que las directivas de la administración para mitigar riesgos al logro de objetivos son llevadas a cabo. Las Actividades de Control son realizadas a todos los niveles de la entidad y en varias etapas del proceso de negocio, y sobre el ambiente de tecnología.”

1.1. Informe COSO II

El Informe COSO II, publicado en el año 2013, brinda un marco integrado de trabajo sobre controles internos sugiriendo, en primera instancia, que los mismos deben estar íntimamente vinculados y direccionados hacia la misión y visión de la compañía. Es así como variarán dependiendo de los objetivos fijados por la alta dirección, el rubro de la compañía y la actividad principal que desarrolle la misma. Estos controles velarán, a su vez, por proteger los activos de la organización.

El Informe COSO II define el control interno como “un proceso llevado a cabo por el Consejo de Administración, la Gerencia y otro personal de la Organización, diseñado para proporcionar una garantía razonable sobre el logro de objetivos relacionados con operaciones, reporte y cumplimiento.”

Pueden encontrarse dentro de este informe básicamente dos requisitos a cumplimentar con los controles implementados: el primero de ellos está estrechamente vinculado a leyes y regulaciones y el segundo a procedimientos, leyes o gobernanza propios de la entidad. Para dar un ejemplo aplicado sobre esto al caso profesional en estudio, podemos observar la presencia de controles para cumplimentar con los requisitos de la Ley Sarbanes Oxley, que habilita a la entidad a cotizar en la bolsa estadounidense, ley sobre la cual nos explayaremos más adelante en este trabajo.

Imagen N° 1: Marco de trabajo - Informe COSO II

Fuente citada: http://www.consejo.org.ar/comisiones/com_43/files/coso_2.pdf

El marco de trabajo de COSO II plantea cinco componentes: el ambiente de control la evaluación de riesgos, las actividades de control, la información y comunicación y el monitoreo. Si bien las cinco disciplinas se encuentran íntimamente ligadas y vinculadas en la práctica, procederemos a describir brevemente cada una de ella para luego, durante el desarrollo del presente

trabajo, focalizarnos en las actividades de control y aplicarlas al ámbito laboral escogido.

Imagen N° 2: Análisis de elementos del marco de trabajo - Informe COSO II.

Fuente citada: http://www.consejo.org.ar/comisiones/com_43/files/coso_2.pdf

El ambiente de control hace referencia a aquello que marca los lineamientos para que las cuatro instancias restantes que componen el proceso puedan ser llevadas a cabo con éxitos. Son directrices que bajan desde el directorio y delimitan los principios rectores de la organización, tanto en la contratación del personal como en el marco laboral que permitirá desarrollar las condiciones propicias para ambientes de control.

La evaluación de los riesgos es la consecuencia natural de la fijación de objetivos. Una vez que estos últimos hayan sido establecidos se debe trabajar en analizar los posibles riesgos a los que esos objetivos se ven sometidos. Quienes hacen el análisis de riesgos deben ser conscientes del dinamismo, tanto

de la organización como del contexto, para ser capaces de administrarlos frente a los cambios.

Las actividades de control, tal como las concibe el Informe COSO II, fueron definidas previamente al comienzo de este capítulo. Sin embargo, agregó sin perjuicio de lo anterior y de manera complementaria, que los controles deben estar alineados con la mitigación de los riesgos que hayan sido previamente evaluados, sean tanto interno como externos.

En los casos de los riesgos internos resulta interesante mencionar el ejemplo de “Data Leak/Loss Prevention” (DLP), el cual hace referencia a la pérdida o fuga de información de alta sensibilidad o confidencialidad desde adentro de la empresa. Sobre la forma en que la empresa en estudio implementa este control nos explayaremos más adelante en el capítulo correspondiente a la descripción de controles relevados.

Otra de las cuestiones a las que hace referencia el informe es a la clasificación de controles en preventivos y correctivos, la segregación de niveles de la organización en cuanto se van a aplicar, y la separación de funciones (registro, aprobación y autorización). Dichos conceptos deben ser mencionados ya que respaldan la operatoria del presente caso de aplicación profesional y se verán aplicados en los controles implementados en "Identidad Privada".

El Informe COSO II, a su vez, hace mención al control sobre la tecnología utilizada en la organización para el cumplimiento de los objetivos. Este punto es de vital importancia ya que el área de seguridad informática operativa vela porque el desempeño de la tecnología acompañe los procesos diarios atados a los objetivos tal como la norma lo sugiere.

Por otro lado, el concepto de gobernanza mencionado en el Informe en cuestión y aplicado en "Identidad Privada" es fundamental para comprender la metodología del desarrollo de los controles en la compañía. Para la mayoría de los controles críticos, existe un documento que establece políticas, normas y procedimiento alineados con los objetivos de la organización que permiten

ejecutar el control de forma uniforme. Por otro lado, todas las áreas implicadas en el proceso, sean usuarios, clientes o proveedores internos tienen el derecho y la obligación de conocer cómo deben actuar frente a esa determinada área.

El documento de gobierno permite identificar a los responsables de la ejecución de las diferentes etapas, para luego poder tomar acciones correctivas en caso de que se haya detectado algún desvío. Una vez finalizado el proceso periódico, la posibilidad de revisar el documento vigente brinda a la organización una oportunidad de mejora.

De acuerdo con el circuito propuesto por esta norma, la información y la comunicación es lo que les da sentido a los procesos de control. Funcionando esta de dos maneras, por un lado, alimenta a la organización de los datos necesarios para poder realizar los controles y por el otro le devuelve a la organización los resultados obtenidos.

La transformación de datos relevantes, tantos internos como externos, en información es vital en el circuito de control y agrega valor a la compañía. La correcta comunicación de los mismos permite la difusión de la tarea y la adopción de medidas correctivas. De acuerdo con el Informe COSO II, para que la información sea de calidad debe ser: accesible, correcta, actualizada, protegida, retenida, suficiente, oportuna, válida y verificable. Por último, la información y comunicación permite efectuar un análisis costo-beneficio que le da sentido al proceso.

El último eslabón del circuito propuesto por el Informe COSO II es el de monitoreo. Esta tarea propone evaluar, de forma conjunta o por separado, cada una de los componentes del control interno a los fines de efectivizar los principios de cada uno de ellos. Se evalúan los hallazgos y se comunican las deficiencias para ser corregidas. Existen también procesos de auditorías internas, evaluaciones, encuestas y otros métodos que colaboran con dicho monitoreo de forma indirecta.

1.2. Norma ISO/IRAM 9001

“El Instituto Argentino de Normalización (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo Argentino de Normalización, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor.” (ISO 9001:2015, 2017)

La norma ISO/IRAM 9001 versa sobre los Requisitos de los Sistemas de Gestión de Calidad para los procesos, productos y servicios.

Siendo una de las tareas fundamentales del área de Seguridad Informática Operativa brindar servicios a clientes internos de la compañía, resulta interesante dar un marco acerca de lo que aporta esta norma al concepto de sistemas de gestión de calidad que brinden una mejor experiencia al usuario final aumentando el grado de satisfacción que el mismo obtiene.

Es así como el enfoque basado en proceso llama la atención ya que aporta una ventaja competitiva al vincular de manera continua los procesos individuales con el sistema de procesos general.

Tal como se menciona en la ISO/IRAM 9001 “Un enfoque de este tipo, cuando se utiliza dentro de un sistema de gestión de la calidad, enfatiza la importancia de:

a) La comprensión y el cumplimiento de los requisitos
b) La necesidad de considerar los procesos en términos que aporten valor
c) La obtención de resultados del desempeño y eficacia del proceso
d) La mejora continua de los procesos con base en mediciones objetivas.”

Ahondando un poco dentro de cada uno de estos puntos, la comprensión y el cumplimiento de los requisitos son esenciales para brindar un servicio de acuerdo a las expectativas que tiene el cliente y a lo que uno mismo como área de servicio se ha comprometido. Si los procesos están integrados y se logran ver de forma sistémica y no individualizada, las posibilidades de que el aprovisionamiento de forma más eficiente aumenta de forma considerable.

Por otro lado, el inciso b) invita a reflexionar sobre el agregado de valor de los procesos que llevamos a cabo. Lo cual es una permite considerar de forma detallada, si cada una de las tareas en la que se vuelva esfuerzo y se invierte recursos agrega valor al proceso en su totalidad. De no ser así, se recomienda que sea reevaluado, modificado y/o eliminado.

Los resultados que dichos procesos le devuelvan a la compañía, deben evidenciar la calidad del desempeño del mismo. Es deseable que se pueda notar la ventaja del enfoque basado en procesos viéndose potenciados los resultados por la integración de cada uno de ellos. Dichos resultados obtenidos deben ser parametrizables para poder ser tabulados y/o normalizados con el objetivo de, en una última instancia, ser medidos.

Si bien la medición de los procesos es una de las etapas finales, no deja de ser de suma importancia y una de las más relevantes. Es aquí donde se verá reflejado en números objetivos y concretos todo el trabajo realizado con anterioridad. En función de estas métricas se podrán tomar decisiones, acciones correctivas y/o preventivas incluso del proceso mismo.

El proceso que propone el paradigma “Plan - Do - Check - Act” es un proceso integrado que se puede aplicar perfectamente a esta metodología donde se finalizará tomando acciones correctivas o preventivas en función de los números que hayan arrojados las mediciones parciales o métricas finales. Comparar el rendimiento de un periodo con otro, puede ser de colaboración para la mejora continua. Adicionalmente, dicha etapa de análisis aportará material para la correcta y enriquecida documentación de los procesos.

1.3. Norma ISO/IEC/IRAM 27001

La norma ISO/IEC/IRAM 27001 se define como “una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (S.G.S.I) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización, tanto propia como datos de terceros.” (ISO 27001, 2018)

Por otro lado, también permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros. Como ocurre con todas las normas ISO, la 27001 es un sistema basado en el ciclo de mejora continua o de Deming.

Similar a lo que plantea la norma ISO 9001 aplicado a procesos, esta norma lo propone aplicado a un Sistema de Gestión de Seguridad de la Información. Teniendo en cuenta que los controles sobre los cuales este trabajo se basa son del área de Seguridad de la Información de una empresa multinacional que responde frente a todos sus “Stakeholder” y debe velar por la seguridad interna, así como por las fronteras con el exterior, queremos focalizarnos en la parte del proceso que le corresponde a la verificación.

La norma propone sobre el SGSI los siguientes pasos:

A. Revisarlo internamente
B. Efectuar auditorías internas sobre el mismo
C. Construir indicadores y métricas
D. Proveer la información obtenida del paso anterior a la dirección para que haga una revisión

Internalizando sobre cómo la norma despliega su postura al respecto, encontramos que, en una primera instancia, determina como crítico la necesidad de definir cuáles son los riesgos y amenazas a los que se ve expuesta una organización. De esta forma será necesario determinar quiénes son los posibles atacantes, a quienes fuera de la compañía les interesa obtener la información

que ella está protegiendo como así también como protegerse de un ataque interno de la compañía.

Por otro lado, habrá que clasificar la información, ordenarla por criticidad, entender quiénes son los dueños de la misma, acordar la asignación de la responsabilidad y hacerles saber fehacientemente que son responsables de velar por ella. El concepto de 100% de seguridad no lo considero posible en un mundo dinámico, cambiante con la emergencia constante de nuevas tecnología y herramientas. Con lo cual considero oportuno contemplar, tal como la norma lo propone, el riesgo residual como aquella brecha que existe entre la seguridad real que se posee en un momento dado y la absoluta.

“Con el objetivo de que cada riesgo identificado previamente quede cubierto y pueda ser auditable, la norma ISO 27001 establece en su última versión: ISO/IEC 27001:2013 hasta 113 puntos de control (en la versión anterior del 2005 eran 133). Los 113 controles están divididos por grandes objetivos:

1. Políticas de seguridad de la información.
2. Controles operacionales.” (ISO 27001, 2018)

Sin embargo, queda a criterio de cada organización añadir más puntos de control de considerarlo necesario, así como customizarlos para adaptarlos a las necesidades específicas que la estructura organizacional o el sector donde la misma desarrolla su actividad principal lo requieran pudiendo diseñar su propio plan de control operacional a la medida de sus necesidades, siempre y cuando no se desvíen de los lineamientos principales de la norma y las buenas practicas.

El área de Seguridad Informática de “Identidad Privada” será la encargada de planificar, ejecutar y controlar el desarrollo de las tareas necesarias para garantizar el cumplimiento de los requisitos de seguridad de la información y para aplicar las acciones que se desprendan del análisis de riesgos realizado en una instancia anterior, el cual mencionamos de forma breve ya que no es tema central de este trabajo, pero hace al contexto.

Según esta norma, es también la organización responsable de hacerle el debido seguimiento a las tareas y procesos que se hayan acordado con terceras partes. Velando por la ejecución de ellas tal lo acordado y tomando las acciones que corresponda ante eventuales desvíos. Puede notarse un ejemplo de esto en el Capítulo IV al describirse el control de Altas, Bajas y Modificaciones de usuarios.

Asimismo, podrá encontrarse un mayor grado de detalle sobre la implementación de los controles recomendados en las buenas prácticas sobre la gestión de la seguridad informática mencionados en la norma ISO/IEC 27002 como complemento y ampliación de la ISO/IEC 27.001. En la primera se detallan catorce dominios principales en donde hacer foco al momento de controlar y gestionar áreas críticas de la gestión, finalizando en una totalidad de 114 controles recomendados.

1.4. Marco de Referencia COBIT 5

“COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las Tecnologías Informáticas (TI) corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.”

Imagen N° 3: Principios de COBIT 5

Fuente citada: https://interpolados.wordpress.com/2016/08/30/cobit-5-unmarco-de-negocio-para-el-gobierno-y-la-gestion-de-las-ti-de-la-empresa/

Sin perjuicio de la importancia de los restantes cuatro principios, considero fundamental para este trabajo hacer foto en el quinto principio que propone separar el gobierno de la gestión. Para poder entender de forma cabal el significado de este principio es fundamental identificar la diferencia entre los conceptos de gobierno y gestión.

Mientras en el marco de COBIT 5 el primero hace alusión a la evaluación de "(...) las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas", el segundo "(..) planifica, construye, ejecuta y controla actividades

alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales".

Teniendo esto en claro, se evidencia que los controles pertenecen al área que gestiona la seguridad informática y que debe estar claramente segregada del área de gobierno para no entorpecer, mutuamente, en sus respectivas tareas. La segregación de estas funciones antes mencionada, no quita la alineación que la gestión debe tener con el gobierno para que reine la coherencia y solidez en las operaciones de la compañía.

1.5. Conclusiones

Los marcos teóricos relevados anteriormente cumplen a los fines de esta tesis tres objetivos básicos: darle al lector una base de conocimiento sobre la cual interpretar los controles descritos en el caso de aplicación profesional, avalar o refutar las prácticas de la compañía "Identidad Privada" y ofrecer una base de normas y/o buenas prácticas para arribar a conclusiones sobre posibles mejoras de los controles tal y como se ejecutan actualmente.

Encuentro importante destacar que el marco de trabajo COBIT 5 ofrece una matriz comparativa donde se puede encontrar la integración de todas las buenas prácticas dentro de TI con COBIT 5. A su vez, es importante aclarar que se ha extraído de los informes, normativas y marcos de referencia relevados los apartados atinentes al caso de estudio.

2. CAPÍTULO II: Análisis del contexto organizacional de la entidad.

Parte del proceso de comprensión de los controles de forma holística, es el conocimiento en detalle del contexto en los que los mismos se diseñan y ejecutan. Los involucrados directos en diseñarlos, sustentarlos, interpretarlos y tomar acciones dentro de la organización son agentes fundamentales. En el próximo capítulo ahondaremos en el contexto organizacional en el cual se encuentra inmerso el presente trabajo de aplicación profesional.

2.1. Introducción

En el presente capítulo se describe la estructura organizacional de la empresa en análisis. Se analizará la organización desde lo macro hacia lo micro llegando al final al área específica en las cuales un analista realiza los controles.

Consideramos que entender el lugar que la seguridad informática ocupa dentro del organigrama, así como sus dependencias y áreas con las que se interrelacionan, son de vital importancia para poder comprender la forma en la que se lleva a cabo la tarea.

El contexto organizacional hace el entorno del área en particular que estamos estudiando, dando al lector una idea de cuál es la idiosincrasia, la importancia que la organización le da al soporte de la tecnología de la información y la seguridad informática en específico.

2.2. Contexto Organizacional de "Identidad Privada"

La empresa analizada, "Identidad Privada", es una empresa líder en el sector metalúrgico con presencia internacional que permanente invierte en el desarrollo y la innovación. Como uno de sus pilares, “buscan minimizar el riesgo para sus clientes y ayudarlos a reducir costos, aumentar la flexibilidad y mejorar los tiempos de entrega. Los empleados de "Identidad Privada" de todo el mundo están comprometidos con la mejora continua y el intercambio de conocimiento a lo largo de una organización global única.”

La misión de "Identidad Privada" es “dar valor a sus clientes”, haciendo hincapié en la calidad de los productos que brinda y entendiendo esta última como la experiencia que el cliente vive al contratar con la empresa. Este concepto de calidad no está estrechamente vinculado al producto en sí mismo que la empresa vende, sino desde la perspectiva integral del proceso (de principio a fin) al contratar con "Identidad Privada". Esta concepción de calidad se mide

exclusivamente desde lo que el cliente expresa y es uno de los pilares fundamentales de la organización.

La empresa tiene un alcance global, tanto en la comercialización de sus productos y en la prestación de sus servicios como en la geolocalización de sus oficinas y plantas productivas. Las oficinas del área de Seguridad Informática de la compañía, se encuentra centralizadas en la Ciudad Autónoma de Buenos Aires, Argentina.

Aproximadamente 50 personas trabajan de forma permanente en el sector de seguridad informática para llevar a cabo las tareas diarias. La labor de la dirección de seguridad informática se divide en tres áreas: Infraestructura, Riesgo y Operaciones. Esta dirección depende a su vez del departamento de Tecnología Informática el cual responde al Director de Finanzas a nivel global.

A su vez la compañía cuenta con un centro de servicios compartidos de tecnología de la información situado en México. El mismo se incorporó a finales del año 2016 con el objetivo de reducir costos debido a la crisis que transitó la empresa por la fuerte baja en el precio del petróleo. En el país México se radicaron las operaciones que, si bien realiza una persona y por el momento no pueden ser automatizadas, son repetitivas y responden a actividades netamente de soporte.

2.3 Gerencia de Seguridad Informática Operativa

Según el autor Herrman Debra, un mal programa de Seguridad Operativa puede deshacer un excelente programa de Seguridad de la Información. La seguridad operativa representa la interacción entre las personas y la tecnología. En línea con este pensamiento, la Seguridad Operativa puede definirse como la implementación de estándares y procedimientos que definen la naturaleza y frecuencia entre usuarios, recursos y sistemas con, a grandes rasgos, dos objetivos: en primer lugar, lograr y mantener un estado seguro del sistema que sea conocido en todo momento y, en segundo lugar, prevenir el robo accidental

o intencional, mal uso, alteración, destrucción o divulgación de información del sistema.

Teniendo en mira estos conceptos teóricos y trataré de describir de forma análoga la realidad práctica en la empresa "Identidad Privada" para lo cual primero haré una breve introducción.

En “Identidad Privada” conviven tres gerencias de Seguridad de la Información, la de Infraestructura y Asesoramiento, la de Riesgos y la Operativa las cuales se retroalimentan en la generación de conocimiento y en la división de tareas. Es importante comprender que el ciclo de seguridad involucra el trabajo coordinado de las tres áreas, donde cada una de ellas ocupa un rol fundamental en el proceso. Para entender cuál es la estrategia de gestión de seguridad de la información no puede verse solo el trabajo de una de las áreas porque el mismo no será comprendido y hasta se correrá el riesgo de desvitalizarlo.

Escapa de los alcances de este trabajo describir y definir la tarea de las áreas de Infraestructura y Asesoramiento, así como la de Riesgos. No obstante, resulta importante dejar en claro que las tareas que desarrolla el área Operativa no son aisladas, sino que trabaja en conjunto, de forma coordinada y sinérgica con las restantes dos áreas.

Una de las funciones del área de Seguridad Informática Operativa es definir qué, cuándo, bajo qué circunstancias y porque las personas en diferentes roles interactúan con los perfiles de Tecnología Informática. Dichas interacciones son documentadas en procedimientos formales que son revisados, ratificados o rectificados y actualizados de manera regular, o después de una actualización o cambio importante en la tecnología y deben ser publicados y accesibles para todos los empleados de la empresa.

Además de las tareas Debra propone en su libro, las cuales son desarrolladas por la gerencia en estudio, la misma también tiene a cargo el desarrollo de la metodología, la definición del alcance, la elección de las herramientas y la

periodicidad de controles sobre las actividades de la organización que apañen a la seguridad de la información.

2.3.1 Área de controles y monitoreo.

El área en la cual se pretende ejecutar el Proyecto de Seguridad Informática, es la relativa a Operaciones. La misma contiene dos coordinaciones: Plataformas; Controles y Monitoreo. La tarea de esta última consiste en el control y monitoreo de los procesos de seguridad que soportan a toda la compañía, así como la propuesta de mejoras, como por ejemplo en la automatización total o parcial de tareas referentes a los controles antes mencionados.

En el área de Controles y Monitoreo trabajan seis personas y una coordinadora. En el área de Plataformas trabajan tres personas y una coordinadora. Ambas áreas están bajo el ámbito de control de una gerente, quien responde al director de seguridad informática.

3. CAPÍTULO III: Identificación de los controles

En las próximas líneas se analizará con mayor detalle la metodología con la que se desarrolla cada uno de los controles seleccionados para este trabajo de aplicación profesional. Se persigue el objetivo de que el lector entienda el propósito por el cual se lleva a cabo el control y el aporte que él mismo hace a la organización, así como las entradas y salidas de datos de los mismos.

3.1. Introducción

En una primera instancia de este capítulo se buscará relacionar los conceptos citados en el marco teórico del presente trabajo con la ejecución práctica de los mismos en la empresa en análisis. Así demostraré cualitativamente el grado de apego con el cual los controles ejecutados se sustentan en las normas y teorías que proponen las buenas prácticas de seguridad informática.

Luego procederá a evaluar los objetivos de llevar a cabo estos controles a nivel general, y no individual de cada uno de ellos. También describiré atributos de los mismos tales como la periodicidad, la alimentación y las herramientas utilizadas para ejecutarlos.

3.2. Aplicación en "Identidad Privada" de los Conceptos Teóricos.

Según demanda y establecimientos de parámetros de las gerencias de Riesgo e Infraestructura hacía con el resto de la compañía y acorde a las medidas de seguridad que se consideren, el área de Controles y Monitoreo desarrolla controles. Estos pretenden cerciorarse que, con la frecuencia que se haya determinado según la demanda y la necesidad de cada proceso crítico sometido a control, los sistemas no fallen y los usuarios no corrompan el horizonte establecido, así como también que las operaciones sean ejecutadas de acuerdo al gobierno y los procedimientos acordados con las múltiples áreas implicadas.

A su vez, "Identidad Privada" cotiza en la bolsa de Estados Unidos con lo cual debe ejecutar los controles establecidos en la “Ley Sarbanes Oxley, tal como lo mencionamos anteriormente haciendo referencia al Informe COSO II “La misma nace con el fin de monitorear a las empresas que cotizan en la bolsa de valores de Nueva york y sus filiales, para evitar fraudes y riesgo de bancarrota, protegiendo al inversor. Así mismo regula las funciones financieras contables y de auditoría, y penaliza el crimen corporativo.

Este monitoreo y control se realiza a través del incremento de los controles internos de las empresas, y la implementación de medidas preventivas que garanticen la integridad y precisión de sus informes financieros.” (Luz, 2015)

Lo cual típicamente significa implementar procedimientos y controles con el fin de que la información financiera y de otro tipo tenga credibilidad. Al igual que un sistema de gestión de calidad, constituye un proceso supervisado por múltiples áreas involucradas en el proceso, una de ellas es la de Seguridad Informática.

3.3. Objetivos

Los controles se realizan con el objetivo de preservar la integridad, confidencialidad y disponibilidad de la información, así como también para remediar en tiempo y forma las posibles fallas que pueden materializarse en el funcionamiento e integración de los sistemas.

Por otro lado, es necesario monitorear el comportamiento del usuario y controlar que su interacción con la información a la que tienen acceso sea acorde a sus funciones y tareas asignadas. Es un fino límite el que establece el acceso a la información por la necesidad laboral y el acceso a la misma para vulnerarla, robarla y/o modificarla.

Por último, los controles se ejecutan también con el objetivo de proveer al usuario el acceso a los sistemas que le corresponde de acuerdo con sus funciones y tareas específicas de forma tal que la disponibilidad de la información está garantizada en tiempo y forma.

3.4. Periodicidad

La periodicidad de los controles es relativa a la criticidad de los mismos y el fin que se persigue con su ejecución, así como también a la actividad a la que estén asociados. Si un control es crítico y tiene un alto impacto, es probable que deba ser ejecutado de forma diaria.

Hay múltiples alternativas frente a la decisión de la frecuencia con la cual establecer la ejecución de un control, enumerare las más utilizadas: mensual, quincenal, semanal, diaria, semestral o a demanda. Esta última alternativa implica que el control se efectuará cuando una acción previa ocurra. Dicha acción dispara la necesidad de que a posteriori se implemente un control sobre la misma para corroborar que haya sido implementada de acuerdo a lo previsto.

El establecimiento de la periodicidad no es algo estático. Se define en un momento determinado con la información disponible, los recursos y sistemas involucrados. Sin embargo, si con el pasar de los meses la situación cambia, la periodicidad puede ser revisada y modificada con una justificación que avale dicho cambio.

3.5. Análisis y recolección de Logs o pistas de auditoría

La recolección de logs para la ejecución de los controles proviene de diferentes herramientas informáticas, sistemas de monitoreo adquiridos por la compañía e incluso áreas que generan información. Entre los más destacados se encuentra el “Security Information and Event Management” (SIEM) el cual disponibiliza una gran cantidad de eventos de los usuarios de la compañía, el “Identity Management” que es un gestor de identidades más otros servicios que exceden a este trabajo, servidores que tienen tareas específicas asignadas y comparten información, el sistema de “ticketing” de la compañía e información que brinda la gerencia de Recursos Humanos en función de altas, bajas y modificaciones de usuarios entre otros.

3.6. Conclusiones

Los parámetros puntualizados en este capítulo aportan la estructura básica que debe contener un control. Sin ellos la entropía que reinaría volvería ineficientes los recursos y la tarea de controlar se tornaría más costosa que beneficiosa.

A modo de conclusión, recomiendo no solo tener en cuenta los parámetros cuantitativos y cualitativos descritos anteriormente sino también los responsables de la ejecución del control con una persona de respaldo entrenada en la tarea, ya que si la misma es crítica y diaria no puede la organización depender de que el único responsable, por ejemplo, nunca se enferme.

No menos importante es que quienes ejecuten los controles deben tener una comprensión global tanto desde la perspectiva de seguridad como desde la del

negocio y/o el usuario final interno para la cual el control se ejecuta. De lo contrario no se podrá medir el impacto y la prioridad del mismo de forma correcta.

4. CAPÍTULO IV: Relevamiento de la entidad analizada

4.1. Descripción de Controles a Relevar

En las próximas líneas se analizará con mayor detalle la metodología utilizada para el desarrollo de cada uno de los controles seleccionados para este trabajo de aplicación profesional. Se persigue el objetivo de que el lector entienda el propósito por el cual se lleva a cabo el control y el aporte que él mismo hace a la organización, así como las entradas y salidas de datos de los mismos.

A su vez, de corresponder, se describirán las herramientas de las que la compañía dispone e intervienen en los controles, como la periodicidad específica de cada uno de ellos.

Por último, se expondrán mejoras que han surgido del relevamiento realizado en virtud de este trabajo.

4.1.1 Procedimiento de Altas, Bajas y Modificaciones de Usuarios.

El área de Seguridad Informática Operativa está a cargo de las bajas, las altas y las modificaciones de todos los usuarios de la compañía con respecto al acceso de los mismo a los sistemas de la organización, ya sean estos últimos de aprovisionamiento manual o automático a través del “Identity Access Management” el cual fue comprado hace dos años atrás y a su vez se contrató un servicio de mantenimiento con la empresa proveedora.

Para poder entender más claramente este control considero oportuno segregar en tres etapas las fases de ejecución del mismo las cuales son, desde el punto

de vista de la seguridad, conceptualmente distintas: las altas, las bajas y las modificaciones de usuarios. Describiré brevemente cada una de ellas y luego ahondar en qué consiste el control.

Entonces la tarea de alta de usuarios atiende desde sus bases al pilar de disponibilidad de la información. Tiene, básicamente, tres enfoques: por una lado pretende ofrecerle al usuario el acceso en tiempo a los sistemas que se aprovisionan de forma automática a través del “Identity Manager”. Esta herramienta colabora con el proceso de alta del usuario teniendo previamente configurado un abanico de perfiles de acuerdo con la posición dentro de la empresa y la categorización de cada uno de ellos por tipo de empleado.

Por ejemplo, no será lo mismo un alta de un empleado para trabajar en la línea de producción de la planta, que un alta de un empleado para las oficinas del proceso contable. Mientras el primero solo requiere dar de alta en la cuenta en el “Active Directory”, al segundo se le debe garantizar además accesos a la Intranet de la compañía “Identidad Privada”, el sistema de mail, chat corporativo y red privada virtual para que pueda conectarse de forma remota.

Siguiendo con el procedimiento, el área de Recursos Humanos informa las altas del día, el “Identity Manager” las recibe y las impacta, mediante procesos automáticos, en cuatro o cinco sistemas dependiendo del perfil del usuario. Este circuito insume, aproximadamente, dos horas de procesamiento computacional y deja listo el perfil del usuario. El objetivo al finalizar es que el usuario cuente con una identidad en “Active Directory” que le permitirá acceder a los recursos mencionados.

Las bajas de usuarios tienen un enfoque completamente distinto desde el punto de vista de seguridad, aunque siguen un proceso a nivel sistema similar. Aquí la prioridad es proteger la información a la cual los usuarios tenían accesos y dejaron de tenerlos por haberse desvinculado de la compañía. Se persigue entonces la correcta desvinculación de los usuarios de todos los sistemas y de las identidades que haya poseído. Téngase en cuenta que, una baja mal ejecutada, le permitiría a un usuario acceder, utilizar y disponer de la información

sin que le correspondiere dejando a la compañía vulnerable ante una posible intención de explotar esa información.

Las modificaciones de usuarios hacen referencia a las licencia, bloqueos o reactivaciones. Las dos primeras tienen un nivel de criticidad similar al de un alta y la última a la de una baja, con la diferencia que las tres son por un periodo de tiempo acotado y no definitivo.

El control de altas se lleva a cabo de forma diaria. Si bien el objetivo es realizarlo de forma preventiva para poder subsanar cualquier desvío para cuando el usuario esté sentado frente a su computadora a primera hora del día luego de ingresar a la compañía, la realidad es que, por un tema de tiempo de procesamiento de sistema, los desvíos se detectan y subsanan de forma correctiva al mismo tiempo que el usuario está arribando.

El control de bajas también se realiza de forma diaria, con el mismo se detectan fallas en los procesos automáticos y se envían a ejecutar de forma manual. Para este control existen también controles compensatorios ya que es de una criticidad alta.

El control de modificaciones está embebido dentro de los controles anteriores según corresponda la medida.

4.1.2 Acceso a Mail y Lync en Tecnología Móvil Correctamente Configurado.

Este control se implementó ya que se detectaron fallas del “Identity Access Management” (I.A.M) en el proceso de alta de los usuarios cuando este debe deshabilitar un grupo del “Active Directory” que les permite a los usuarios tener acceso al mail y el sistema de chat de la compañía desde cualquier dispositivo móvil.

Por defecto todos los usuarios se dan de alta con este grupo habilitado y debe correrse un proceso especial para deshabilitarlos. Sin embargo, en algunas

ocasiones el I.A.M. falla en la ejecución de este proceso y algunos usuarios permanecen con el grupo habilitado.

Debido a que la utilización del mail de la compañía, así como también del canal de chat asociado en los dispositivos móviles debe ser autorizado expresamente por un director de la organización y los dispositivos en los que se utilizan deben cumplir con ciertos requisitos previamente establecidos por el área de seguridad, es un punto de falla que quede el protocolo habilitado sin las debidas autorizaciones.

Como menciono anteriormente, en algunos casos por un error de sistema los usuarios quedan incorporados al grupo de “Active Directory” que los habilita a usar ambos servicios sin haber pasado por las etapas de autorización correspondientes y es en este caso donde se debe implementar un exhaustivo control.

Por tal razón de forma semanal se toma la totalidad de nuevos usuarios para detectar aquellas personas que pertenecen a cualquiera de estos dos grupos, y por ende están habilitados para utilizar los servicios desde un dispositivo móvil que no sea la computadora que provee la empresa, pero no tienen las autorizaciones correspondientes. Una vez detectados aquellos desvíos que produce la falla del sistema que administra las identidades, se procede a quitarlos de los grupos de forma manual y a evaluar por medio de un comando si durante el tiempo que estuvieron habilitados sin que les correspondiere explotaron la falla del sistema utilizando los servicios.

De esta forma, con un control correctivo se rectifica el error que produjo el I.A.M y también se considera si la falla que el usuario podría haber explotado fue efectivamente aprovechada o no para poder tomar las medidas correspondientes.

4.1.3 Supervisión de empleados externos

Este control pretende cerciorarse que cada empleado externo, es decir que no es de la planta permanente de la empresa, posea un supervisor asignado en los sistemas con el fin de poder atender todas las necesidades que como usuario tiene el contratado y que dependen de la aprobación del supervisor.

El circuito de alta, baja y asignación de supervisores de los empleados que no son propios de la compañía, sino contratados a través de una consultora, no se hace de forma automática a través del “Identity Access Manager” (I.A.M.) según lo que informa el área de recursos humanos, sino que la solicitud llega por medio de un ticket que es ejecutado por un centro de servicios compartidos que posee la compañía en el país de México.

Sucede a menudo que los supervisores de los empleados externos abandonan la compañía, cambian de función o nunca son asignados. Esta acefalía a la cual quedan expuestos quienes son externos produce inconvenientes a la hora de gestionar roles, permisos, renovaciones, extensiones de plazos y/o autorizaciones para las cuales el sistema debe consultar al supervisor antes de asignarlas.

Debido a la cantidad de inconvenientes que traía que no haya un supervisor cargado y a la dificultad para proceder con las solicitudes que involucran a personal externo, se decidió implementar un control quincenal que detecta a los terceros que no tienen supervisor asignado. La idea original era que una vez identificado los desvíos se procediera a enviar un mail informando de la situación irregular en la que se encuentra el empleado y se solicita que por favor se regularice.

4.1.4 Prevención de Filtración o Fuga de Información

Para poder entender este control es necesario hacer una previa introducción a la clasificación de la información que posee la compañía. Podemos así encontrarnos con cuatro categorías:

- Altamente Confidencial

- Confidencial
- De Uso Interno ● Pública

La información que está clasificada como Altamente Confidencial requiere de un seguimiento diario acerca de las consulta, accesos y descargas que se hacen sobre ella, ya que son parte neurálgica del negocio y le brindan a la organización una ventaja competitiva respecto de sus competidores en el mercado.

Más allá de que los permisos que se necesitan para acceder a ella tengan un circuito minucioso de solicitud, aprobación y asignación, así como responsables de evaluar si la tarea que realiza el solicitante o el puesto que ocupa amerita acceder a ella o no, por la criticidad y el alto impacto que un descuido de esa información puede producir en el negocio, se han implementado controles diarios a pedido del área que evalúa los Riesgos de la seguridad de la información.

Es así como se llevan adelante dos controles diarios que tienen por objetivo final evitar que haya filtraciones de información altamente confidencial y que también hacen un monitoreo de eventuales comportamientos anómalo que puedan suceder.

La información que está clasificada como altamente confidencial es monitoreada por un “Security Information Event Manager” (SIEM) el cual está configurado para enviar una alerta automática al supervisor de la persona que haya accedido al archivo, la carpeta compartida o el sitio de la intranet que contiene la información más de cinco veces en una hora o más de veinticinco veces en un día.

El supervisor recibe la alerta con el formato estándar del área de Riesgos en la cual se le solicita que no hay riesgo detectado o que si lo hay.

Es en función de este procedimiento que se realizan dos controles. El primero de ellos consiste en registrar todas las alertas automáticas que han sido enviadas donde se detalla la fecha del evento, la persona que accedió a la información, el supervisor de la misma, el área al que pertenece, el sitio al que accedió, entre

los datos más relevantes. Pero fundamentalmente se controla y se deja registrado si el supervisor respondió que se detectó un riesgo o no.

En segundo lugar, se realiza un control para corroborar que todos los eventos que detectó el SIEM salieron automáticamente. Más de una vez se detecta que el SIEM falla y es necesario enviar la alerta de forma manual.

4.1.5 Control de Tráfico de Internet

El control de tráfico de internet se realiza de forma mensual, su ejecución lleva aproximadamente dos semanas de trabajo con un recurso medio tiempo disponibilizado exclusivamente. Devuelve un reporte que es utilizado como base de datos para el posterior análisis pormenorizado y detallado del comportamiento del usuario frente al tráfico de datos.

El reporte arroja la cantidad de datos descargados y subidos a internet de los usuarios de todas las unidades de negocios del grupo económico. Una vez obtenida esta información se genera una lista segregada de los diez usuarios que se destacaron en cada una de estas categorías: carga y descarga. A continuación, los supervisores y jefes de los usuarios son informados de dicho comportamiento anómalo y cada uno de ellos es responsable de tomar las medidas que considere necesarias.

Es importante destacar que este primer reporte solo contiene la cantidad de datos, no así el contenido al que el usuario accedió como también que está limitado al uso de internet que el empleado haya hecho desde la red de la compañía quedando excluida la conexión por red privada virtual.

Generalmente lo que ocurre es que los supervisores solicitan un detalle pormenorizados de la calidad de los datos a los que los usuarios accedieron, es decir aquella información que hayan descargado o subido a internet.

Dicho control se ejecuta con el fin de identificar posibles fugas de información a través de la subida de información a internet o de proteger los activos de la

compañía con descargas que resulten potencialmente peligrosas. Por otro lado, altos volúmenes de consumo son llamativos en cuanto al comportamiento habitual que tiene el empleado y la empresa considera en sus políticas que debe ser monitoreado ya que puede colaborar en el cuidado de la información de la compañía. Tanto se trate de ser accedida como de ser compartida.

4.2 Resumen de Controles Analizados

Tabla Nª 1: Comparación de Controles Relevados

	Objetivo	**Periodicidad**	**Herramientas Involucradas**
Alta, Baja y Modificación de Usuarios	Garantizar la vinculación o desvinculación de los usuarios con los sistemas básicos de acceso a la compañía en tiempo y forma	Diaria	Identity Manager
Acceso a Exchange y Lync en dispositivo móvil	Verificar que quienes puedan acceder al sistema de mail y chat de la compañía desde un dispositivo móvil tengan la debida autorización	Quincenal	Identity Manager, Consola de Comandos y Active Directory.
Supervisión de empleados externos	Asignar un supervisor a aquellos empleados externos que no lo tengan con el fin de no entorpecer la operatoria diaria de los sistemas	Semanal	Identity Manager
Fuga de Información	Proteger la información clasificada como Altamente Confidencial de posibles fugas internas.	Diaria	SIEM

Tráfico de Internet	Informar y controlar la cantidad de datos cargados o descargados hacia y desde internet desde las redes de la compañía.	Mensual	Logs

4.3 Recomendaciones

El control referente a las altas, bajas y modificaciones de usuarios no estaba contemplando previo al desarrollo de este trabajo de aplicación profesional, por un lado, el universo total de las aplicaciones en las que debían impactar las medidas. Por otro lado, tampoco estaba teniendo en consideración la intervención en el proceso del “Identity Manager”, el cual produce fallas en la réplica de los accesos al conectarse con aplicaciones.

La elaboración de este relevamiento allanó el camino para idear un control que apunta a monitorear estas tareas de forma integral e incluso superadora incluyendo a los empleados externos de la compañía.

En cuanto al control de mail y Lync en tecnología móvil se detectó que, si bien una vez realizado el control se regulariza el estado del usuario, podría implementarse un paso más al finalizarse el control que garantizara que la vulnerabilidad no haya sido explotada. Es así como se coordinó con el área que se ocupa de la tecnología “Exchange” para correr un comando que devolviese la información acerca de si el usuario había utilizado el protocolo durante la brecha de seguridad producida entre la falla del sistema y la detección por medio del control.

Quizás uno de los casos más atractivos sea el control de supervisores de empleados terceros, el cual pasó a ser despreciable una vez implementado este trabajo profesional ya que se pudo detectar que la mayoría de los desvíos que

arrojaba este control se debía a casos recurrentes que no atendían las notificaciones.

En función de esto, se informó a la gerencia y se decidió asignarle al usuario un supervisor que se corresponda con el jefe de su último supervisor o la persona que haya solicitado su alta. De esta manera los casos recurrentes dejaron de aparecer y los desvíos del control se redujeron en un 80%.

Adicionalmente el control arrojó información acerca de la actitud de los empleados externos, quienes obviaban el mail de alerta y no tomaban medidas ante la solicitud de asignación de un supervisor.

Con lo cual el área de Seguridad Informativa Operativa, apoyándose en los resultados arrojados, decidió incluir una instancia más en este control. La misma conlleva la asignación de un supervisor de acuerdo a las siguientes premisas:

a) Se asignará la persona que solicite el alta del empleado. En caso de que no esté en la compañía o haya rotado de función
b) Se asignará el jefe del ultimo supervisor asignado al tercero.

De esta forma el universo de empleados terceros sin supervisor asignado ha ido disminuyendo sustancialmente al punto que los desvíos se han vuelto más fáciles de controlar y remediar.

Conclusiones Finales

Los controles que realiza el área de seguridad informática operativa buscan garantizar que los servicios ofrecidos dentro de una estructura organizacional pensada para brindar soporte al resto de la compañía, se realicen de forma eficiente cumpliendo con los estándares establecidos y los niveles de aprovisionamiento de servicio de alta calidad en tiempos adecuados para el usuario.

Los controles que se refieren a cuentas de usuarios finales, tanto el de altas, bajas y modificaciones como el de la asignación de los supervisores a los terceros persiguen garantizarles el servicio a que el "Identity Access Management" debe ser brindarles de forma automática.

Los controles sobre prevención de fuga de información y tráfico de internet tienen otro nivel de criticidad ya que no están asociados a un manejo de los sistemas; y en relación con el control de telefonía se asimila a un control compensatorio de una falla del sistema. Ambos representan un desafío para mejorar la experiencia de los usuarios para a proteger a la compañía de posibles amenazas generadas por los usuarios internos.

Haber podido relevar los controles para este trabajo de investigación implico conocer en profundidad cada uno de los procesos, las herramientas y los actores implicados en ellos. En el camino de construcción del mismo, "Identidad Privada" ha recibido de mi parte sugerencia sobre mejora en su ejecución.

El área de tecnología en general y el de seguridad en particular, se ven en el constante desafío de mejorar sus tiempos de respuesta. A esta tarea se le suma, para el área de seguridad informática específicamente, no resultar un obstáculo a la hora de implementar una nueva herramienta, utilizar una nueva aplicación,

realizar una actualización, comprar un programa, innovar con nuevas tecnologías como la nube o la internet de las cosas.

Para ser una empresa de vanguardia que considera la calidad como sinónimo de la satisfacción del cliente se debe poder responder con celeridad a los cambios tecnológicos del entorno. Es por esto que el diseño de la estructura de la seguridad informática está pensado para que cada área tenga segregada las tareas fundamentales y pueda responder de forma articulada a los pedidos internos que luego tendrán un impacto directo al servicio final que la compañía entregue.

Los controles y el monitoreo que efectúa el área atinente a este trabajo de aplicación profesional persiguen en su rutina objetivos tales como la automatización de los mismos para poder responder de forma más segura y eficiente y permitiéndole abarcar nuevos tópicos. A su vez persiguen también la detección de irregularidades, la capacidad de análisis de los resultados que estos controles arrojan y la posibilidad de mejorar la experiencia del usuario interno de la compañía entre otros.

Este trabajo busca explotar los resultados obtenidos para poder proponer formas innovadoras que mejoren el aprovisionamiento de un servicio. Eliminar controles que solo verifican que la tarea de una herramienta informática que debería ser automática se haya efectuado correctamente no suma valor a la cadena de tecnología ni a la de custodia de la información.

El área de Seguridad Informática Operativa se ocupa diariamente de procurar que la información esté protegida, que los sistemas cumplan con el nivel de servicio comprometido, como también para poder mejorarlo interpretando los resultados de los controles.

La autora del presente trabajo, considera importante implementar métricas sobre estos controles para contribuir a utilidad de los mismos, que magnifiquen los desvíos, que permitan entender las causas raíces y tomar consecuentes

decisiones para erradicar el control, mejorar el servicio o proponer caminos alternativos.

Conocer sobre seguridad informática, entender cuáles son los objetivos que persigue, proteger la información, así como el negocio en sí mismo es fundamental para poder desarrollar esta tarea. Este trabajo de aplicación profesional ha colaborado con el círculo virtuoso del análisis y el entendimiento cabal para poder aportar formas alternativas de resolver la tarea. Pretende que este sea el camino que se persiga para el crecimiento del área y la mejora del servicio.

Los controles por sí solos no aportan más que la garantía de que la tarea fue hecha tal lo planeado, y la empresa espera de sus profesionales mucho más que eso.

Bibliografía

ISO/IEC 27001:2017, I. (2015). *Tenología de la Información - Sistema de Gestión de Seguridad de la Información - Requisitos.* IRAM .

Auditool. (2 de Febrero de 2017). Obtenido de https://www.auditool.org/blog/controlinterno/2651-lo-que-todo-auditor-debe-conocer-de-sox

CMMI. (08 de Julio de 2018). Obtenido de Modelo CMMI de Madurez: http://www.allsoft.mx/recursos/ElModeloCMMI.pdf

Herrmann, D. S. (2007). *Complete Guide to Security and Privacy Metrics .* New York, United State of America: Auerbach Publications.

Informe COSO II. (24 de Agosto de 2018). Obtenido de Consejo Profesional de Ciencias Economicas: http://www.consejo.org.ar/comisiones/com_43/files/coso_2.pdf ISACA. (2012). *COBIT 5.* ISACA.

ISO 27001. (25 de Octubre de 2018). Obtenido de S.G.S.I: https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridadinformacion.pdf

ISO 9001:2015. (30 de Noviembre de 2017). Obtenido de http://rode.com.ar/wpcontent/uploads/2017/11/ISO-9001.-2015.pdf

Jaquith, A. (2007). *Security metrics : replacing fear, uncertainty, and doubt.* Indiana, United States of America: Addison-Wesley.

Luz, s. D. (19 de Marzo de 2015). *RedesZone*. Obtenido de SIEM: https://www.redeszone.net/2015/03/19/que-son-las-soluciones-siem-para-laseguridad-interna-de-una-empresa/