UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS
ESCUELA DE INGENIERÍA INFORMÁTICA

PROPUESTA PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LOS SERVICIOS EN LA NUBE, APOYADO EN LA NORMA ISO/IEC 27017: 2020 PARA LA EMPRESA PRICOSE, PRIMERA SOCIEDAD AGENCIA DE SEGUROS S.A, UBICADO EN GUADALUPE, SAN JOSÉ

PROYECTO DE GRADUACIÓN PARA OPTAR POR EL GRADO DE LICENCIATURA EN INGENIERÍA INFORMÁTICA CON ÉNFASIS EN GERENCIA

KARLA ARAYA RIVERA

AUTORA

DANIEL ÁLVAREZ GARRO

TUTOR

OLMAN NÚÑEZ PERALTA

LECTOR

San José, Costa Rica

Diciembre, 2021

CONTENIDO

TABLAS

FIGURAS

GRÁFICOS

RESUMEN EJECUTIVO

La computación en la nube se crea para suministrar a las organizaciones de cuantiosos volúmenes de almacenamiento, de esta forma los usuarios confían en los proveedores de servicios y en que este se hará cargo de la seguridad que los recursos deben tener, con lo cual se pierde la destreza de mantener resguardados los datos. Tal es el caso de PRICOSE, Primera Sociedad Agencia de Seguros S.A, en donde, avanzando de la mano con la tecnología, lograron trasladar sus recursos a la nube de Azure; sin embargo, no existe alguna garantía sobre la disponibilidad, confidencialidad e integridad de los datos trabajados y alojados en esta.

El proyecto presentado a continuación, está enfocado en la norma ISO 27017, cuyo propósito es diseñar una propuesta para implementar la seguridad de la información de los servicios en la nube, con el fin de identificar amenazas de acceso, clasificar la información, formar los roles y responsabilidades con respecto a la seguridad y, finalmente, con los datos obtenidos; realizar una serie de políticas sobre el uso y manejo de la información para obtener el resguardo de los tres pilares fundamentales de la seguridad de los datos.

Para el desarrollo de este proyecto, se definió trabajar sobre un enfoque mixto, ejecutando una encuesta a los empleados de la organización, una entrevista al encargado del departamento de Tecnologías de la Información y aplicando técnicas de observación al servicio de la nube de Azure; además, del estudio de la norma de seguridad ISO 27017. Se llegó así a la conclusión del logro del diseño de la propuesta para PRICOSE con el fin de implementar la seguridad de la información y a su vez, procurar como principal recomendación, la aplicación de las normas de seguridad planteadas.

CAPÍTULO I: INTRODUCCIÓN

Debido al gran avance tecnológico, la información de las empresas puede llegar a almacenarse en un espacio virtual para acceder a ella en todo momento y desde cualquier lugar, ya sea por medio de un computador, un móvil o una tableta, esto, con solo el hecho de tener una conexión a internet. La computación en la nube o lo también llamado servicios en la nube, tiene como su función principal ofrecer a sus consumidores, ya sea individuos o empresas de todos los tamaños, una gran cantidad de recursos en donde se maneja la información de un modo seguro, con excelente y constante mantenimiento, al alcance y momento de cuando la persona así lo requiera.

Es necesario que estos avances vayan de la mano del desafío constante que cada empresa tiene para garantizar la tranquilidad de los clientes ante la información brindada; la seguridad de la información se ha convertido en uno de los principales pilares de las labores de hoy en día; así como es importante la seguridad física, es igual de importante la seguridad sobre la información que se da, la cual no es tangible, pero puede llegar a exponerse a situaciones vulnerables.

Planteamiento del problema

Los servicios en la nube son un nuevo modelo que permite brindar productos a través de internet, mediante sitios web, ello significa que dichos valores ya no se encuentran alojados de manera física en las empresas; por el contrario, son los proveedores externos quienes se hacen cargo de la plataforma o infraestructura requerida, lo cual ofrece al cliente el alojamiento de la información de toda la organización y a su disposición a través de la conectividad de internet.

PRICOSE Primera Sociedad Agencia de Seguros, S.A., es una empresa dedicada a la comercialización de seguros. Gracias a su solidez, confianza, proyección y prestigio, PRICOSE ha logrado un importante posicionamiento en el mercado y aunado a ello, ha sido meritoria de un sinfín de reconocimientos por parte de su único proveedor, el Instituto Nacional de Seguros (INS). Cuenta con 136 asesores en seguros tanto dentro como fuera del GAM y ofrece una gran cantidad de productos a sus clientes (PRICOSE, 2017).

Debido a su constante crecimiento, PRICOSE se vio en la necesidad de hacer una transformación del negocio para realizar la mayoría de sus funciones de forma

digital; dentro de sus cambios, está la migración de sus datos y sistemas principales a la nube, fue así como se decidió por una plataforma que le ofreciera diferentes servicios y herramientas integradas como lo es la nube de Azure; sin embargo, el cambio se dio de forma repentina y se detectaron algunas situaciones importantes que pueden generar riesgos a la organización, dentro de estas situaciones se pueden mencionar:

- No existe garantía para la integridad, disponibilidad y confidencialidad de la información alojada en la nube. Es de vital importancia proteger los datos personales como financieros que la organización posee.
- No cuenta con una apropiada identificación de los riesgos de la información guardada en la nube. La empresa desconoce cuáles y cuántos tipos de riesgos se puedan estar dando.
- No existe una administración de activos. Falta de organización y planeación con el manejo de la información que se encuentran en la nube, no hay pautas a seguir para la debida gestión que se le tenga que dar a la información.
- No existen roles adecuados para cada funcionario de TI. No se cuenta con personal que ejecute funciones en pro de la seguridad de la información; debido a esto, podrían existir vulnerabilidades sobre la información que se encuentra alojada en la nube.
- Inexistencia de una política para los empleados, sobre el manejo y uso de la información, lo que provoca un desconocimiento del cómo manejar los distintos tipos de datos que se manipulan en cada departamento de la empresa.
- Falta de controles por parte de la empresa sobre los servicios contratados. El personal de TI de la empresa no tiene la información clara de que tipo de recursos se manejan en la nube y dejan la responsabilidad completa en su proveedor.

Objetivos

En el siguiente apartado se indicarán los objetivos, tanto el general como los específicos, para el desarrollo de la propuesta.

Objetivo general.

Diseñar una propuesta para implementar la seguridad de la información de los servicios en la nube, apoyado en la Norma ISO 27017:2020 para PRICOSE.

Objetivos específicos.

- Concienciar al personal de TI sobre las normas de seguridad para la información alojada en la nube.
- Identificar las amenazas de acceso, divulgación o modificación de información que se presentan en la organización basado en la norma ISO 27017.
- Clasificar la información de acuerdo con su orden de sensibilidad según la norma ISO 27017.
- Establecer políticas sobre el uso que se le da a la información y la forma en que será compartida basado en la norma ISO 27017.
- Formar los roles y responsabilidades internas en la compañía, con respecto a la seguridad de la información hospedada en la nube.

Justificación

El contar con una norma de seguridad para controlar los servicios hospedados en la nube, hoy en día, se vuelve un tema de gran importancia en cualquier tipo de organización. Es necesario tener claras las funciones y responsabilidades de cada involucrado, sean proveedores o clientes, para que el manejo de la información se lleve con la seguridad que amerite.

Con la seguridad de la información en la nube, PRICOSE pretende amparar los datos que tienen a disposición por medio de internet y limita así el acceso, exclusivamente, a usuarios que estén autorizados.

A partir de lo anterior, PRICOSE tiene la necesidad de contar con un método de gestión de seguridad de la información alojada en la nube y, mediante una serie de controles, garantizar la seguridad de lo más importante que tiene cualquier empresa

como lo es la información; lo anterior, apoyado con un marco de referencia mundial, la norma ISO 27017: 2020.

Viabilidades

A continuación, se mencionan las viabilidades tomadas en cuenta, con el fin de analizar las probabilidades necesarias para que el desarrollo de la propuesta sea llevado a cabo con el éxito esperado.

Viabilidad técnica.

Con este tipo de viabilidad se descubrirá si las propiedades tecnológicas que se tomarán en cuenta son las adecuadas para desenvolver la investigación. Para la implementación de lo propuesta se utilizará un equipo portátil con las siguientes características:

- Hardware.
    - Portátil LENOVO.
    - Procesador Intel I7.
    - Memoria de 12 Gb.
    - Disco Estado Sólido 240Gb
    - Disco Duro de 1 Terabyte.

- Software.
    - Sistema Operativo Windows 10 PRO.
    - Adobe Reader.
    - Adobe Acrobat.
    - Paquete de Office 365.

Se toman en cuenta las propiedades del equipo que la empresa brindará para elaborar el trabajo; asimismo, la investigación es documental y con las características anteriormente mencionadas, se demuestra que cubriría la perspectiva técnica para ejecutar las funciones, sin mayores inconvenientes.

Viabilidad operativa.

La viabilidad operativa es la que indica si el plan propuesto cumple con las expectativas del negocio; al respecto, es importante validar si se cuenta con el respaldo de la empresa y si será necesario algún tipo de instrucción para la ejecución de la propuesta.

En este caso, se cuenta con el apoyo de la Gerencia para la propuesta de una norma que llegue a cerrar las brechas de seguridad presentes en la organización.

Se debe tomar en cuenta que el departamento de TI cuenta con poco conocimiento en cuanto a normativas de seguridad, por lo que, luego de realizada la propuesta, se debe capacitar al personal para la comprensión de la normativa indicada, pues todo el personal involucrado debe tener claro el objetivo que se pretende alcanzar y de esta forma efectuar la implementación.

Viabilidad económica.

La viabilidad económica muestra que se deben tener los recursos económicos necesarios para la propuesta, teniendo en cuenta que más allá de un costo, se debe obtener un beneficio para la organización.

La empresa cuenta con los recursos de hardware y software para el desarrollo de la propuesta por lo cual no se incurriría en estos gastos. Debido a que la empresa se encuentra realizando teletrabajo con todo el personal, se debe contar con una conexión a internet para la investigación correspondiente. En el caso de la normativa ISO 27017, el costo será asumido por el estudiante, dicha herramienta será comprada mediante la página de INTECO con un valor de 34.020,30 colones.

Según lo indicado por el Ministerio de Trabajo y Seguridad Social (2021) en el apartado de lista de salarios mínimos por ocupación año 2021, el costo de un Bachiller Universitario es el de ¢ 568 819.86 mensual, lo anterior, de acuerdo con lo publicado en la Gaceta del 06 de enero. Dicho salario es por jornada ordinaria, lo que representa un total de 192 horas mensuales, para un monto de ¢ 2 962.60 por hora.

Para el desarrollo del proyecto, se dedicará un total de 112 horas mensuales, equivalentes a un monto de ¢ 331 811.2 mensual.

Viabilidad legal.

La viabilidad legal hace referencia al actuar con respecto a las leyes, siempre buscando que los procesos a elaborar y desempeñar se amparen bajo el cumplimiento de ellas, evitando cualquier riesgo de delito por alguna infracción. Las normativas ISO a nivel internacional aportan múltiples beneficios a las organizaciones, con ellas se certifica el buen funcionamiento que tiene cada departamento dentro de la organización. Aplicar la norma ISO 27017 en PRICOSE no tendría ningún efecto negativo, por el contrario, sería un modelo para seguir en muchas aseguradoras del país, alcanzando las buenas prácticas de seguridad de la información.

De igual forma se tomaron en cuenta tres leyes de Costa Rica para analizarlas y determinar la factibilidad en este ámbito:

Delitos informáticos (Ley 9048). El objetivo de esta ley es amparar tanto a las personas físicas como jurídicas. Se forman modificaciones al Código Penal donde rigen delitos penales como lo son la suplantación de identidad, espionaje informático, instalación o propagación de programas informáticos maliciosos, suplantación de páginas electrónicas, facilitación del delito informático.

Reprimir y sancionar delitos informáticos (Ley 8148). Ley que comprende la violación de comunicaciones electrónicas, fraude informático, alteración de datos y sabotaje informático. Orientado al no uso de información de terceros con el fin de obtener un beneficio personal.

Protección de datos (Ley 8968). En dicha ley se cubre la autodeterminación informática, principio del consentimiento informado, principio de calidad de la información, derechos que le asisten a la persona, entre otros artículos. El fin de dicha ley es proteger a todas las personas indiferentemente de la nacionalidad, domicilio o residencia, el respeto a sus derechos fundamentales.

Para la elaboración de esta propuesta, se dispone de la información con consentimiento y autorización de la empresa; adicional a ello, se tiene conocimiento y respeto por las leyes antes mencionadas, por lo que se tiene la factibilidad necesaria para la elaboración de la propuesta.

Proyecciones

Para realizar la propuesta de implementación, se tomará como referencia la normativa ISO 27017, con esta se espera como resultado, una serie de lineamientos y controles que permitan crear oportunidades de mejora, con respecto a la forma en que se maneja la seguridad de los datos en la organización.

Con esta propuesta, se pretende alcanzar el mayor grado de madurez a nivel organizacional para que se pueda implementar la seguridad de la información en la empresa; mediante los análisis por desarrollar, se intenta concienciar a los empleados sobre el correcto uso de la información y de los activos de la empresa. Adicional a ello, se pretende crear una cultura al departamento de TI y a las altas gerencias, sobre la importancia que amerita la seguridad de los datos; el objetivo es poner en evidencia los hechos que se pueden optimizar en cuanto a la seguridad de los datos presentes en la nube.

Alcance

El alcance de la propuesta es aplicado a toda la información y los servicios hospedados en la nube. Se cubre el manejo de la información, la administración de sus activos, así como el control hacia el personal. Dicha propuesta es exclusiva para la empresa PRICOSE.

Asimismo, dicha propuesta es a nivel documental por lo que no se llevará a cabo ninguna programación, aunque sí se indicarán los elementos técnicos que se deben abarcar.

Con la intención de proponer una implementación de un conjunto de políticas y procedimientos a seguir en cuanto a la seguridad de la información alojada en la nube, la propuesta se fundamenta en el estándar de la Norma ISO 27017 según los siguientes apartados:

- Políticas de seguridad de la información. En este apartado se deberán concretar todas las responsabilidades a seguir en cuanto a la seguridad, con esto se certifica a la organización de la confidencialidad, disponibilidad como integridad de la información. Se indicará la frecuencia de revisión de las políticas, además de verificar que se estén ejecutando según lo establecido; se deberá asignar los responsables de velar por dicho cumplimiento.

- Organización de la seguridad de la información. La información se segmentará según su valor y sensibilidad para la organización. Se controlará todo el proceso de implementación y operación de la seguridad de la información y de sus activos, se definirá y controlará la asignación de las responsabilidades que tiene la organización con respecto al manejo de la información.
- Administración de activos. Se identificarán los activos presentes (máquinas virtuales, fuentes de almacenamiento, bases de datos, aplicaciones, cuentas de correo, Active Directory, páginas web), se realizará un inventario y sobre dichos activos, se asignarán los responsables de su manejo y administración.
- Controles de acceso. Se establecerá una política sobre los controles de acceso basada tanto en los requisitos de seguridad como del negocio. Se definirá de forma clara, cuáles serán los permisos y las limitaciones que le correspondan a cada usuario, dependiendo de las funciones que le compete; además de los procedimientos a seguir para la eliminación de usuarios, así como el manejo con la gestión de contraseñas.
- Seguridad de las operaciones. Se documentarán los procedimientos de operación que se la dará a la información guardada en la nube. Se elaborará una bitácora para identificar los cambios realizados, donde se puedan auditar y controlar los procesos que sufrieron alguna alteración, conocer a quienes pueden afectar, entre otros datos importantes para la adecuada administración de la información; además de validar los ambientes de programación de desarrollo y pruebas, se deben definir los controles por seguir para el manejo de dichos ambientes.
- Seguridad de las comunicaciones. Se elaborará un documento donde se registren los intentos de ataques o acciones no autorizadas en la nube. Se propondrán procedimientos para accesos seguros, qué puertos mantener abiertos o cerrados, entre otros.
- Adquisición, desarrollo y mantenimiento de los sistemas de información. Se elaborará un documento con las políticas por seguir para la adquisición o desarrollo de software que se encuentren en la nube, además de definir controles en las aplicaciones para la seguridad de la información que se maneje en cada sistema.

- Política de seguridad de la información de la relación con proveedores. Se confeccionarán los lineamientos que rigen para el proveedor del servicio en la nube.
- Aspectos de la seguridad de la información en la continuidad del negocio. Se identificarán los eventos que generen dificultades a los procesos del negocio, junto con el impacto y consecuencias en donde estén atentando la seguridad de la información. Sobre los eventos presentados, se desarrollará un documento como plan de recuperación del negocio para asegurar la disponibilidad de la información.
- Cumplimiento con los requisitos legales. Se delimitarán cuáles serán los derechos y obligaciones de cada usuario sobre la utilización de la información que cada uno maneja, además de realizar los procedimientos apropiados para el cumplimiento de dichas restricciones con el propósito de velar por la protección y privacidad de los datos.
- Funciones y responsabilidades compartidas dentro de un entorno de computación en la nube. Se identificarán cuáles son las responsabilidades que tiene tanto el proveedor como la organización sobre el manejo de la información.
- Eliminación de activos del cliente del servicio en la nube. Se realizarán los procedimientos por seguir sobre la utilización o eliminación de los activos que la organización maneje en la plataforma brindada por el proveedor.
- Monitoreo de servicios en la nube. Se realizará un documento como método de revisión continua, con periodos definidos para asegurar la continuidad del servicio, además de fijar al personal adecuado y autorizado para la realización de dichas funciones.
- Alineación de la gestión de la seguridad para redes virtuales y físicas. Se establecerán los controles de entrada para los servicios manejados en la nube, así como la definición de los límites de acceso.
- Se elaborarán los procedimientos, políticas y lineamientos necesarios para los puntos anteriores.

CAPÍTULO II: MARCO DE REFERENCIA

En el presente capítulo se detallarán los temas esenciales para desenvolver la base teórica de la investigación, se ampliarán los conceptos fundamentales con respecto a la seguridad de los datos, la información en la nube y la normativa que se tomó como referencia, para lograr así una mejor comprensión, al momento de desarrollar la investigación.

PRICOSE Primera Sociedad Agencia de Seguros, S.A., es una empresa dedicada a la comercialización de seguros. En 1996 se dio su nacimiento, a consecuencia de un nuevo modelo de negocio de seguros que surgió en el país. La principal causa de su origen fue el deseo de establecer una organización con un sector numeroso de agentes de seguros, para lograr proyectarse como una de las empresas líderes en este mercado.

Cuenta con 136 asesores en seguros tanto dentro como fuera del GAM, ofrece una cantidad significativa de productos y de esta forma, construye una cartera importante de clientes, por lo que, la propuesta para la seguridad de la información basada en la nube velará por la integridad, confidencialidad y disponibilidad de esta información (PRICOSE, 2017).

Uno de los activos más importantes para PRICOSE, así como para la mayoría de las organizaciones es la información. Según Goñi (2000) el término de información es definido de la siguiente manera:

> La información es el significado que otorgan las personas a las cosas. Los datos se perciben mediante los sentidos, estos los integran y generan la información necesaria para el conocimiento quien permite tomar decisiones para realizar las acciones cotidianas que aseguran la existencia social. El ser humano ha logrado simbolizar los datos en forma representativa, para posibilitar el conocimiento de algo concreto y creó las formas de almacenar y utilizar el conocimiento representado. La información en sí misma, como la palabra, es al mismo tiempo significado y significante, este último es el soporte material o simbología que registra o encierra el significado, el contenido (párr. 13).

ISOTools Excellence (2021) se refiere a tres tipos de información con las que debe trabajar cualquier organización para llevar adecuadamente, el amparo de los datos, sin importar el sector en que se desarrolle o la actividad que ejerza:

> Crítica. La información crítica es la que es indispensable para el correcto funcionamiento de la organización y sus operaciones. La información crítica es la que establece los beneficios de la organización a medio y largo plazo, ya que facilitará las ventas y el servicio al cliente. Conocer la información y los datos son necesarios para establecer todos los protocolos de seguridad necesarios para su protección.
>
> Valiosa. Tiene un alto componente subjetivo y lo que para una organización es información valiosa, para otra puede no serlo, ya que depende de la actividad y el sector. No toda la información y datos tienen el mismo valor y las empresas deben analizar cuáles son necesarios y cuáles no para el funcionamiento de negocio.
>
> Sensible. La información es sensible en el sentido de que es información privada de los clientes de la organización y, por lo tanto, solo tiene que tener [sic] acceso a las mismas personas autorizadas. Los sistemas de seguridad de la información tienen que garantizar la protección de datos de los clientes (párr. 14).

Asimismo, para dar la importancia que la información merece, García (2020) expone que, primeramente, se debe conocer el tipo de datos que se maneja, para clasificarlos y hallar la mejor manera de protegerlos, pues también es importante entender que la información debe ser preservada en todo su ciclo de vida, desde que se crea hasta que se destruye y para esa protección, este autor hace referencia al cubrimiento de las siguientes fases:

> Inventarios de activos de información: es preciso identificar toda la información que se maneja e inventariarlos registrando todos los datos necesarios para su gestión como pueden ser: tamaño, ubicación, servicios en los que se usa, departamentos, personas responsables, etc.
>
> Criterios de clasificación de la información: es necesario establecer una clasificación de la información disponible basada en criterios, tales como nivel de accesibilidad, confidencialidad, utilidad, funcionalidad, impacto…

Etiquetado de la información: cada activo identificado, en función de la clasificación que se haya determinado, debe etiquetarse para que, de este modo, se identifique el nivel de protección que precisa el activo.

Medidas de seguridad disponibles: necesitamos conocer las medidas de seguridad que se aplican en la organización que puedan emplearse en la protección de la información. Medidas como pueda ser cifrado de información, sistemas de copias de seguridad, sistemas de control de accesos, … Esto nos dará una visión del esfuerzo que pueda suponer proteger nuestra información.

Determinación de medidas de seguridad: en función de la clasificación establecida se debe construir una matriz que establezca las medidas de seguridad que se deben aplicar a cada nivel de dicha clasificación en cada una de las fases del ciclo de vida de la información.

Implantación de medidas de seguridad: con la información identificada, clasificada y etiquetada, lo siguiente es implantar las medidas de seguridad que han determinado para cada activo de información.

Seguimiento y control: para evitar brechas de seguridad, es preciso que realicemos seguimiento y auditorías de seguridad que verifique el estado y el cumplimiento de las medidas de seguridad implantadas (párr. 17).

Al ver la importancia que tiene la información en la organización, comprendiendo que es un activo más y que con ella se logra mantener la operativa del negocio, se deduce que resguardarla es de las principales razones del porqué en los últimos años, se ha tomado con mayor responsabilidad su seguridad. Según comenta Areitio (2008) respecto de la seguridad:

La seguridad ha pasado de utilizarse para preservar los datos clasificados del gobierno en cuestiones militares o diplomáticas, a tener una aplicación de dimensiones inimaginables y creciente que incluye transacciones financieras, acuerdos contractuales, información personal, archivos médicos, comercio y negocios por internet, domótica, inteligencia ambiental y computación ubicua. Por ello, se hace imprescindible que las necesidades de seguridad potenciales sean tenidas en cuenta y se determinen para todo tipo de aplicaciones.

La seguridad de los sistemas de información es una disciplina en continua evolución. La meta final de la seguridad es permitir que una organización

> cumpla con todos sus objetivos de negocio o misión, implementando sistemas que tengan un especial cuidado y consideración hacia los riesgos relativos a las TIC de la organización, a sus socios comerciales, clientes, Administración Pública, suministradores, etc. (p.2).

Dando continuidad a lo antes mencionado, se entiende que la seguridad de la información se ha convertido en un segmento esencial para que las organizaciones ejecuten sus operaciones con los menores riesgos informáticos posibles; se debe tener presente que de alguna forma, es inevitable proteger en un 100% a las empresas de los ataques cibernéticos, pero la seguridad debe enfrentar dichos riesgos y la mejor manera de hacerlo es manteniendo un análisis constante, logrando detectar a tiempo cualquier situación anormal y con ello, prevenir o bien, de ser necesario, poder actuar en el momento adecuado.

Como se ha mencionado anteriormente, la propuesta ante la implementación de la seguridad de la información hospedada en la nube es para resguardar los tres pilares esenciales en que se asienta la información, pilares que según ISOTools Excellence (2018) se detallan a continuación:

- Disponibilidad: la información siempre debe estar accesible para el momento en que se pueda requerir. Dentro de las consideraciones por seguir para poder avalar la integridad de los datos están:
    - Controlar los sistemas de información con el fin de implementar políticas para el buen funcionamiento de los datos.
    - Efectuar sistemas de control de cambios para verificar si hubo algún cambio con la información.
    - Recuperación de la información por medio de respaldos, esto ante cualquier eventualidad ocurrida.
- Integridad: la información debe ser verídica, correcta sin alteraciones ni errores.
- Confidencialidad: este pilar hace referencia a que únicamente el personal autorizado es el que puede acceder a dicha información.

  Como principales recursos para certificar la confidencialidad de la información:

- Autenticación de usuarios: con este control se puede asegurar que la persona que tiene el ingreso a los sistemas o información es el usuario que en efecto debe ser.
- Cifrado de información: se convierten los accesos de una manera cifrada para evitar que la información pueda verse reflejada por personas no autorizadas.
- Gestión de privilegios: permite dar acceso a las carpetas, documentos o información de una manera específica, según el tipo de usuario.

En la figura No.1 se muestra cómo se integran en un solo ciclo, los pilares de la información. Se deja en evidencia que los tres son igual de importantes para el buen uso y manejo de los datos.

Figura 1. Pilares de la información.

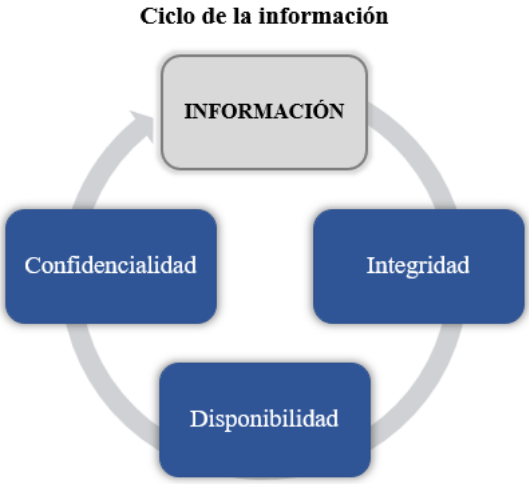

Figura 1. Pilares de la información.
Elaboración propia (2021).

De igual forma, así lo certifica la ISO 27001 (ISO, s. f.) cuando indica que la seguridad de la información habita en la conservación de su confidencialidad, integridad y disponibilidad, dentro de una organización.

Para contar con estos tres pilares, también se debe pensar en mecanismos para el control de acceso, entendido este como la posibilidad de otorgar permisos a uno o más usuarios con el fin de ingresar a la información de la organización. El control de acceso incluye tres conceptos esenciales: la identificación, la autenticación y la autorización. La identificación se ejemplifica cuando un usuario muestra su identidad al sistema,

normalmente puede usarse un identificador de usuarios. La autenticación es la forma en que se pueda validar que el usuario que está tratando de tener acceso es el correcto, utilizando técnicas para realizar esas validaciones como lo es la contraseña o bien, una huella digital y la autorización, es el permiso que se le dio al usuario para acceder a los diferentes sistemas o carpetas según los privilegios con los que cuente (Drozhzhin, 2020).

Los componentes de gestión de acceso encierran la tecnología, métodos y personas que admiten establecer de forma automatizada y coordinada las siguientes tareas, según lo dicho por el Instituto Nacional de Ciberseguridad (2015):

> "Proveer y gestionar las cuentas de usuario, identidades y contraseñas
> Administrar los flujos de trabajo para la aprobación de la creación, modificación,
> Suspensión y eliminación de cuentas de usuario
> La provisión, revocación, auditoría, etc. de roles y permisos
> Realizar auditorías e informes" (párr. 3).

El manejo de la información, según su tipo y los mecanismos indicados, van de la mano con el conjunto de técnicas que se utilizan para hacer cumplir las normas de seguridad de la información en la nube establecida. Una adecuada configuración de los privilegios con los que puede contar cualquier usuario, debe ser una parte fundamental con el fin de darle la mayor protección a los datos, ante los accesos no autorizados y ante las vulnerabilidades a las cuales puede estar expuesta la información de la empresa. Con el fin de poder detectar las vulnerabilidades para corregirlas a tiempo o bien disminuirlas. Respecto al término de vulnerabilidad, Areitio (2008) comenta que:

> La vulnerabilidad puede entenderse también como la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo. Las vulnerabilidades asociadas a los activos incluyen las debilidades en el nivel físico sobre la organización, los procedimientos, el personal, la gestión, la administración, los equipos, el software o la información (p. 23).

Quiroz y Marcías (2017) mencionan que hay tres tipos de vulnerabilidades diferenciadoras en los sistemas: las vulnerabilidades sobre los sistemas instalados que ya son de la comprensión de las empresas desarrolladoras y en las que ya está la solución; las vulnerabilidades que también son conocidas, pero con sistemas que aún no han sido instalados ni implementados; sin embargo, la empresa desarrolladora no actúa sobre lo no instalado, y las vulnerabilidades que aún no han sido identificadas por la empresa, provocaría una amenaza en la organización, si alguna persona externa a la empresa, se diera cuenta de estas debilidades.

Las vulnerabilidades presentes en PRICOSE, como bien se ejemplificó en la sección planteamiento del problema, pueden iniciar una cadena de amenazas, las cuales atenten contra la calidad de la información. Como amenaza Solarte, Enríquez y Benavides (2015), mencionan:

> Las amenazas informáticas están relacionadas con la posibilidad de que algún tipo de evento se pueda presentar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial sobre los activos informáticos y los sistemas de información. Las amenazas son consideradas como los ataques cometidos por personas internas o externas, que pueden ocasionar daños a la infraestructura tecnológica, a los sistemas de información o a la misma información que circula en la organización.
>
> Las amenazas pueden presentarse por acciones criminales en las que intervienen seres humanos violando las normas y las leyes, o sucesos de orden físico por eventos naturales que se puede presentar, o aquellos eventos en los que el ser humano propicia las condiciones para determinar un hecho físico, o por negligencia que son las omisiones, decisiones o acciones que pueden presentar algunas personas por desconocimiento, falta de capacitación y/o abuso de autoridad (p. 498).

En este sentido, Tarazona (2007) explica que las amenazas se pueden agrupar en cuatro grandes categorías que son: los factores humanos (tanto errores como accidentales); fallas en los sistemas de información, desastres naturales (terremotos, temblores, etc.) y por medio de actos realizados de forma perversa. Además de ello, Tarazona (2007), expone algunas de las amenazas más frecuentes:

Spywre (Programas espías): código malicioso cuyo principal objetivo es recoger información sobre las actividades de un usuario en un computador (tendencias de navegación), para permitir el despliegue sin autorización en ventanas emergentes de propaganda de mercadeo, o para robar información personal (p.ej. números de tarjetas de crédito).

Troyanos, virus y gusanos: son programas de código malicioso, que de diferentes maneras se alojan el los [sic] computadores con el propósito de permitir el acceso no autorizado a un atacante, o permitir el control de forma remota de los sistemas.

Phishing: es un ataque del tipo ingeniería social, cuyo objetivo principal es obtener de manera fraudulenta datos confidenciales de un usuario, especialmente financieros, aprovechando la confianza que éste tiene en los servicios tecnológicos, el desconocimiento de la forma en que operan y la oferta de servicios en algunos casos con pobres medidas de seguridad.

Spam: recibo de mensajes no solicitados, principalmente por correo electrónico, cuyo propósito es difundir grandes cantidades de mensajes comerciales o propagandísticos. Se han presentado casos en los que los envíos se hacen a sistemas de telefonía celular mensajes de texto, o a sistemas de faxes.

Botnets (Redes de robots): son máquinas infectadas y controladas remotamente, que se comportan como "zombis", quedando incorporadas a redes distribuidas de computadores llamados robot, los cuales envían de forma masiva mensajes de correo "spam" o código malicioso, con el objetivo de atacar otros sistemas; se han detectado redes de más de 200.000 nodos enlazados y más de 10.000 formas diferentes de patrones de *"*bots*"*.

Trashing*:* un método cuyo nombre hace referencia al manejo de la basura. No es una técnica relacionada directamente con los sistemas de información, pues los atacantes se valen de otra forma de ingeniería social y para ello, el mecanismo utilizado, es la búsqueda en las canecas de la basura o en los sitios donde se desechan papeles y documentos de extractos bancarios, facturas, recibos, borradores de documentos, etc., y posteriormente utilizarla según convenga, elaborando un perfil de la víctima para robar su identidad, o teniendo acceso directamente a la información que se suponía confidencial (pp. 138 - 140).

Cualquiera de estos u otros tipos de amenazas que no son atendidas de manera oportuna, pueden ocasionar riesgos para los sistemas y los datos de la organización, ocasionando de esta forma, daños irreparables y presentando efectos negativos de importancia. Para Areitio (2008):

> El riesgo es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio (o conjunto de activos) o en toda la organización. Este impacto se puede producir debido a que una amenaza explote vulnerabilidades para causar pérdidas o daños.
>
> Un entorno de riesgo es aquél en el que una amenaza concreta o un grupo de amenazas, pueden explotar una vulnerabilidad o grupo de vulnerabilidades determinado, exponiendo los activos a daños o perdidas.
>
> El riesgo se caracteriza por una combinación de dos factores: la probabilidad de que ocurra el incidente no deseado y su impacto (p. 24).

Por lo anterior, es que se deben considerar una serie de normas o políticas creadas con el fin de evitar o bien, prevenir situaciones difíciles dentro de las empresas, y fijar de forma clara todas aquellas responsabilidades de los diferentes tipos de usuarios, sean administradores, usuarios finales, directivos y, demás perfiles existentes en la organización.

Referente a políticas informáticas, se toma como el canal que se da formalmente, entre los usuarios y la organización, para que por medio de medidas establecidas se indiquen las pautas a seguir para el manejo de la información, sistemas, entre otros aspectos de interés, con el objetivo de preservar y asegurar los medios en que se comunican los datos compartidos. Para Rodríguez y Ribón (2019) las políticas de seguridad informática deben considerar los siguientes elementos:

> Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
>
> Objetivos de la política y descripción clara de los elementos involucrados en su definición.
>
> Responsabilidades por cada uno de los servicios y recursos informáticos aplicados a todos los niveles de la organización.

> Requerimientos mínimos para la configuración de la seguridad de los sistemas que abarca el alcance de la política.
> Definición de violaciones y sanciones por no cumplir con las políticas.
> Responsabilidades de los usuarios con respecto a la información a la que tiene acceso (pp. 5-6).

Estas políticas o normas mencionadas son definidas por el Organismo Internacional de Estandarización (ISO). ISO se deriva del griego *isos*, cuyo significado es "igual" y lo que se da a entender es que, indiferentemente del país y del idioma siempre son ISO. Las normas ISO se componen de una serie de pautas, con el fin de gestionar de una manera adecuada la organización en sus diferentes ámbitos, pueden ser aprovechadas en cualquier tipo de empresa y hoy en día, se cuenta con 23 849 normas internacionales (ISO, s. f.). Según referencia de ISOTools (2021) sobre las normas:

> Las normas ISO son un conjunto de normas orientadas a ordenar la gestión de una empresa en sus distintos ámbitos. La alta competencia internacional acentuada por los procesos globalizadores de la economía y el mercado y el poder e importancia que ha ido tomando la figura y la opinión de los consumidores, ha propiciado que dichas normas, pese a su carácter voluntario, hayan ido ganando un gran reconocimiento y aceptación internacional (párr. 1).

De igual forma, ISOTools Excellence (2021) hace referencia a una lista de ventajas que las organizaciones pueden obtener al implementar cualquiera de las normas que la ISO tiene a disposición:

- Al implementarlas, agrega valor agregado en cuanto a la calidad, seguridad y confiabilidad.
- Menor tiempo en el descubrimiento de problemas.
- Una mayor satisfacción por parte de los clientes.
- Una mayor intervención de los colaboradores de la organización.
- Mejor agudeza para detectar las necesidades de los clientes.
- Facilidad hacia la capacitación de los empleados.
- Mejor posicionamiento de la empresa.
- Ayuda a la relación con los proveedores, entre otras.

La propuesta para la implementación de la norma de seguridad ISO 27017 a PRICOSE, trae consigo ventajas significativas como empresa comercial, con lo cual se favorece el conocimiento y las mejores prácticas con los principales expertos a nivel mundial.

Dentro de las normas ISO se crea la serie 27000 en donde se muestra la forma en que las organizaciones pueden establecer un sistema de gestión de seguridad de la información (SGSI). A partir de las normas más destacadas para la gestión de la seguridad de la información en la nube:

ISO / IEC 27000. Esta norma muestra las principales bases sobre la importancia de la implantación del SGSI (Sistema de Gestión de Seguridad de la Información) así como los caminos a seguir para el establecimiento, monitorización, mantenimiento y mejora de un SGSI. Es aplicable a cualquier tipo y tamaño de empresa. (ISO, s. f). Cada política se representa con una enumeración dentro de la misma serie; para la ISO 27000 se ahondará en las normas:

- ISO / IEC 27001. Se caracteriza dentro de las normas de mayor importancia, domina los requisitos del sistema de gestión de seguridad de la información y del tratamiento de riesgos, la seguridad de la información forma parte del tratamiento de los riesgos de la empresa; estos requisitos se basan en establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI), además; enumera los objetivos de control que desarrolla la ISO 27002: 2005. La mayor parte de la implementación de esta norma se basa en fijar las políticas organizacionales para prevenir infracciones a la seguridad tanto para el hardware como para el software que mantiene la organización. La seguridad de la información forma parte del tratamiento de los riesgos de la empresa (ISO, s. f).

En la figura No. 2, se refleja que la ISO 27001 se basa en la gestión del riesgo, primeramente, localizándolo, para luego asegurar las medidas.

Figura 2. Estructura de la Norma ISO 27001.

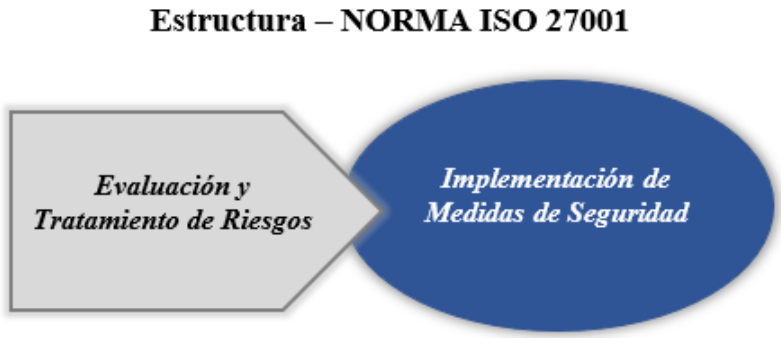

Figura 2. Estructura de la norma ISO 27001.
Elaboración propia (2021).

- ISO / IEC 27002. Estándar relacionado concretamente con la seguridad de la información; desde la seguridad de las redes y las TI hasta las documentaciones y datos informáticos, incluye la selección, implementación y gestión de controles, siempre tomando en cuenta los riesgos. Pensada para aquellas organizaciones que:
    - Intentan elegir controles en el proceso de implementación de un SGSI;
    - Ejecutar controles de seguridad normalmente aceptados y
    - Pretenden desenvolver sus propios modelos de gestión de seguridad de la información (ISO, s. f.).

A continuación, se detalla y se analiza la norma principal de esta indagación (ISO 27017), política que ayudará en el desarrollo de la investigación y que se planteará a la organización para una mejora en los procedimientos realizados, con el fin de asegurar la información alojada en la nube:

- ISO 27017. Publicada en diciembre de 2015. Es la norma de seguridad para la computación en la nube, complementada con la norma ISO 27002. Propone una serie de reglas para la gestión de la seguridad de la información de los servicios en la nube. Está diseñada tanto para los clientes como a los proveedores de servicios en la nube, nivelando y aclarando la relación de responsabilidad y de funciones que se da entre ambos, con el propósito de ayudar a que los servicios en la nube estén igual de protegidos como lo están el resto de los datos que se encuentran alojados de forma física (ISO, s. f.).

Esta norma ofrece 37 controles en la nube, orientados en la ISO / IEC 27002 y adicional a ellos, ofrece siete controles más que trabajan los siguientes puntos:

- Responsabilidades entre el proveedor del servicio en la nube y entre el cliente.
- Tanto la eliminación como la devolución de activos cuando un contrato se resuelve.
- La protección del ambiente virtual del cliente.
- Lo que atañe a la configuración de una máquina virtual.
- Instrucciones administrativas que están relacionadas con el ambiente en la nube.
- Seguimiento de la actividad de clientes en la nube.
- Por último, la alineación del entorno de la red virtual y la nube.

Dentro de los beneficios presentes en las compañías al aplicar la serie 27017, está en que el responsable del departamento de tecnologías de la información pueda mitigar los riesgos existentes, toma de decisiones más oportunas ante el tipo de información que se deberá migrar a la nube, una mejor gestión sobre los contratos de prestación de servicios en la nube, además de asegurar las responsabilidades que deba cumplir cada parte (Ingertec, 2020, párr. 1).

Flores (2021) comenta en su artículo, que la ISO 27017 ha logrado tener el mismo éxito y aceptación en la industria de tecnologías de la información, que la ISO 27000. Para las empresas que brindan sus servicios totalmente en la nube ha sido de gran afinidad, con lo cual logran resguardar todos los ángulos de seguridad en este ambiente, y con ello, distinguirse en el mercado, madurando y al mismo tiempo, formando un modelo de computación en la nube que les asegura un ahorro de dinero y de tiempo.

Profundizando en el tema, la llamada computación en la nube es una tecnología que ofrece una variedad de servicios especializados como lo son: administración de redes, almacenamiento, servidores, software; todo a través de sistemas de internet, lo cual trae un potencial para la innovación en los departamentos de tecnologías de la información de las distintas organizaciones, independientemente del mercado en que se desenvuelven. Arias (2015) define de la siguiente manera la computación en la nube:

> Podemos definir el cloud computing como un sistema de computación distribuido orientado al consumidor, que consiste en una colección de ordenadores virtualizados e interconectados que son suministrados dinámicamente y presentados como uno o más recursos computacionales unificados, conforme acuerdo de nivel de servicio negociado entre el proveedor de servicios y el consumidor (p. 13).

La computación en la nube tiene características muy marcadas con respecto al uso de las aplicaciones y servicios en las organizaciones, Hernández y Florez (2014) mencionan una serie de características:

- Autoservicio. El cliente tiene la opción de poder asignar, eliminar o aumentar servicios de los que cuenta la nube, sin tener que realizar una solicitud a su proveedor, evidentemente, para ello se requiere tener de un perfil con privilegios.
- Acceso a la red. En el momento en que se desea o bien se necesita, el cliente puede acceder a su información en la nube por medio de la plataforma que se le brinda a la organización.
- Rapidez y flexibilidad. Los clientes pueden adquirir la cantidad de capacidad que requieran, en el tiempo en que se necesite e inclusive por un lapso definido para cumplir con tareas específicas.
- Servicio controlado. Cada proveedor de servicio en la nube supervisa los recursos y el uso que se les da a ellos, la mayoría de estas tareas son gestionadas de forma automática por parte de los proveedores por medio de evaluaciones que realizan de manera rigurosa.
- Escalabilidad. Tanto la arquitectura como los sistemas con los que cuentan los proveedores de servicios en la nube, son predecibles y eficientes, logrando minimizar cuellos de botella y tiempos de espera.
- Virtualización. El cliente puede tener acceso a las plataformas en la nube, independiente del hardware y sistemas operativos que utilicen (Unix, Max, Windows, etc.), por lo que la información tendrá siempre las mismas características.

- Seguridad. El proveedor es el encargado de cifrar los datos que el cliente comparte en su plataforma.
- Disponibilidad de la información. Los datos siempre estarán a disposición de la(s) persona(s) que lo ocupen, siempre y cuando, se tenga acceso a internet y con la debida autorización.

Los productos brindados, por medio de la computación en la nube, están diferenciados por tres clases. Woorsluys (2011), Garg y Buyya (2012) citado por Arias (2015), describen esos grupos:

> **Infraesructure As a Service (IaaS):** en este nivel son ofrecidos los recursos como servidores, almacenamiento y comunicación en forma de servicios. El usuario puede administrar estos recursos instalando software, añadiendo discos virtuales, configurando usuarios y permisos, etc. El EC2 de Amazon Web Services es un ejemplo de este tipo de servicio con recursos como el escalamiento automático e importación de máquinas virtuales del usuario.
>
> **Platform As a Service (PaaS):** en este nivel los proveedores de cloud computing ofrecen un entorno de desarrollo para que el usuario pueda crear y alojar sus propias aplicaciones y distribuirlas como servicio sin tener que preocuparse de la infraestructura que necesita.
>
> Este entorno incluye también componentes que pueden ser incluidos en las aplicaciones y servicios para monitorizarlos y gestionarlos. El Windows Azure de Microsoft es un ejemplo de este tipo de servicio.
>
> **Software As a Service (SaaS):** en este nivel las aplicaciones son distribuidas como servicios y accedidos por demanda. En este modelo los usuarios no necesitan mantener la infraestructura propia ni instalar software, ya que la aplicación y sus datos asociados son accedidos por medio de Internet, mediante un navegador que puede ejecutar en un cliente ligero. Este modelo, además de liberar al usuario de toda complejidad, permite disminuir considerablemente los precios, visto que el proveedor puede diluir los costes compartiendo la aplicación con un gran número de usuarios. Google Apps es un ejemplo de este tipo de servicios (pp. 14-15).

Definir el presupuesto que se tiene en la organización para implementar servicios en la nube, es sin duda uno de los factores para determinar qué tipo de sistema a implantar se adecua al negocio: lasS, PaaS o SaaS. Conforme las organizaciones desenvuelven sus estrategias para lograr efectuar la computación en la nube, dentro de las decisiones por tomar, está la de analizar si se les saca partida a las ventajas de una nube pública o bien, si la mejor elección está en hacer la implementación sobre una nube privada; ademásde tomar en cuenta los recursos y funcionalidades que se necesiten y de esta forma, buscar los proveedores que lo ofrezcan. Según Hernández (2014) existen cuatro modelos en los que se extienden los servicios en la nube:

Nube pública. Aquellas organizaciones que venden servicios en la nube pero que colocan su infraestructura públicamente por medio de internet.

Nube privada. Es colocada para una empresa o tercero en específico, está fuera de las instalaciones y dentro de ella con el fin de proporcionar servicios de TI a usuarios internos. Se tendría un mejor manejo de los recursos, pero al ser físicos se convierte en limitada.

Nube comunitaria. Intervenida por varias organizaciones, pero siguiendo los mismos objetivos como las políticas, requisitos entre otros. Tramitada por las empresas o por un tercero y de igual forma puedan estar fuera y dentro de las instalaciones.

Nube híbrida. Admite la movilidad de datos y aplicaciones entre una o más nubes (privada, comunitaria o pública), los entes están divididos, pero identificados con una misma tecnología.

La integración de la nube es una labor que requiere de estudio y ejecución de cambios para la adaptación a las funciones específicas que se ocupen. Las organizaciones deben de enfocarse en analizar cuál de los servicios de nube se ajusta mejor con su escenario de ambiente local, ambiente multinube y su contorno. Los modelos de negocio se aplican tanto a los consumidores como a los proveedores en la nube. Aguilar (2012) menciona las siguientes soluciones en las que los proveedores de la nube se enfocan:

- Los servicios de la nube proporcionan la red e infraestructuras de computación mediante plataformas y soluciones. Los proveedores de servicios y soluciones de la nube son similares, y permiten desarrollar y proporcionar servicios y soluciones de la nube desde la perspectiva de los consumidores. Los proveedores de servicios de la nube incluyen organizaciones que operan con centros de datos propios y apoyados en servicios de virtualización. Los proveedores son variados y tienen gran implantación, aprovechando sus centros de datos y de su experiencia en alojamiento de datos y aplicaciones.
- Proveedor de servicios de plataformas de la nube. Proporcionan plataformas basadas en la nube, hospedados en entornos de sistemas e infraestructuras específicos, para que los desarrolladores puedan acceder a la plataforma, desarrollar una nueva aplicación de negocios y alojarlas en la plataforma basada en la nube.
- Proveedores de tecnologías. Desarrollan las herramientas y tecnologías que facilitan que la nube se establezca y se suministre a los consumidores de recursos proporcionados por la nube. Ofrecen un amplio rango de herramientas, tecnologías, sistemas operativos para facilitar el despliegue de nubes públicas, privadas, híbridas y comunitarias.
- Proveedores de soluciones. Desarrollan aplicaciones o suites completas, para conseguir un amplio mercado de consumidores de la nube (otras operadoras de telefonía e internet).
- Modelos de negocio para consumidores. Estas empresas aplican conceptos de la nube a sus estrategias de negocios. Ofrecen soluciones para gestión empresarial (p.96).

Según lo ejemplificado por los autores sobre el concepto de computación en la nube, se puede abreviar que, mediante esta tecnología, se logra proporcionar cualquier servicio en un progreso de infraestructura anticipadamente virtualizada.

La virtualización, según Red Hat (2021) es un mecanismo primordial para el progreso inmejorable de la computación en la nube; esta tecnología permite que un recurso efectúe la función de varias tareas, mientras que la computación en la nube admite un conjunto de recursos suministrados automáticamente. Los programas de virtualización son cada vez más manejados por las empresas, por lo que se han

convertido en materiales necesarios para el trabajo diario. La empresa Vmware (2021) hace referencia al término de virtualización, de la siguiente manera:

> La virtualización consiste en crear una representación basada en software, o virtual, de una entidad física como, por ejemplo, aplicaciones, servidores, redes y almacenamiento virtuales. Es la forma más eficaz de reducir los gastos de TI y a la vez, aumentar la eficiencia y la agilidad para empresas de cualquier tamaño.
> La virtualización puede mejorar la agilidad, la flexibilidad y la escalabilidad de la infraestructura de TI, a la vez que permite disfrutar de unos ahorros importantes. Algunas ventajas de la virtualización, como la mayor movilidad de las cargas de trabajo, el aumento del rendimiento y de la disponibilidad de los recursos o la automatización de las operaciones, simplifican la gestión de la infraestructura de TI y permiten reducir los costes de propiedad y operativos (párr. 1-2).

Además, la empresa Conzultek (s. f.) hace referencia a los tipos de virtualización que ejecutan funciones distintas en un servicio completo:

> **Virtualización del sistema operativo:** se implementa para ejecutar más de un sistema operativo en el mismo dispositivo.
> **Virtualización del servidor:** esta es una de las áreas donde inicia el mundo de la virtualización y consiste en correr máquinas virtuales con sistemas operativos de versión de servidor. Cada máquina virtual ejecuta un sistema operativo independiente de las demás. Ejecutar más de un servidor en el mismo servidor físico.
> **Virtualización de almacenamiento:** es un conjunto de dispositivos físicos y lógicos que aparentan ser una única unidad de almacenamiento que permiten almacenar la información de las aplicaciones, servicios y usuarios. El almacenamiento en la nube es el medio más utilizado en la virtualización de almacenamiento.
> **Virtualización de red:** es la capacidad de combinar recursos físicos y lógicos de red de manera que se vean como una unidad.
> **Virtualización gráfica**: se presenta como un mercado emergente y funcional. Básicamente consiste en usar gráficos en la nube. Por ejemplo, de la misma manera en que accedemos a nuestras fotos en la nube, podemos trabajar con

aceleración GPU (Unidad de Procesamiento Gráfico) de forma remota, sin tener que poseer físicamente un equipo como estación de trabajo.

Virtualización de aplicaciones: permite encapsular las aplicaciones de manera que no se requiera la instalación de aplicaciones sobre el sistema operativo. Permite ejecutar aplicaciones corporativas que están hospedadas en un servidor compartido.

Virtualización de perfil: mediante esta virtualización, el usuario tiene acceso a su perfil, documentos y configuración del escritorio de manera que estos estén disponibles cuando este cambie de estación de trabajo. Esto quiere decir que su información no está ligada a una estación específica.

Virtualización de escritorios: conocida como VDI (siglas en inglés de Virtual Desktop Infrastructure). La infraestructura de virtualización del escritorio lo que busca es ejecutar escritorios corporativos en el equipo del cliente o en forma centralizada el Centro de Datos.

En cuanto a lo mencionado anteriormente y resumiendo, se entiende como virtualización a la tecnología en donde se pueden formar ambientes variados, simulados o bien, recursos dedicados desde un único hardware físico. Se necesita del software "hipervisor", que se conecta directamente con el hardware para fraccionar un sistema en ambientes separados, diferentes y seguros, conocidos como "máquinas virtuales".

Cuando se habla de máquinas virtuales, se hace referencia a la ejecución de un software en equipos físicos, conformada por un conjunto de archivos, en donde se utiliza los recursos de memoria, CPU, disco del equipo físico, para que entre en funcionamiento la máquina virtual y está, a la vez, su sistema operativo; cubren las mismas funcionalidades como si se tratara de una máquina normal, sin embargo, son los archivos informáticos los que se ejecutan y permiten que se trabajen de forma independiente.

Sobre el concepto de máquina virtual, la empresa VMware (2021) detalla:

Una máquina virtual es un sistema informático virtual, es decir, un contenedor de software bien aislado que incluye un sistema operativo y una aplicación. Cada máquina virtual autónoma es completamente independiente. Si se instalan varias máquinas virtuales en un mismo ordenador, es posible ejecutar varios sistemas operativos y aplicaciones en un solo servidor físico o «host».

Una capa ligera de software, llamada «hipervisor», desvincula las máquinas virtuales del host y asigna recursos informáticos de forma dinámica a cada máquina virtual según las necesidades. Las máquinas virtuales tienen las siguientes características, que ofrecen varias ventajas:

Creación de particiones

Ejecute varios sistemas operativos en una sola máquina física.

Distribuya los recursos del sistema entre las máquinas virtuales.

Aislamiento

Permita aislar la seguridad y los fallos en el nivel de hardware.

Garantice el rendimiento gracias a los controles avanzados de recursos.

Encapsulación

Guarde el estado completo de una máquina virtual en archivos.

Transfiera y copie máquinas virtuales con la misma facilidad que si fueran archivos.

Independencia del hardware

Suministre o migre cualquier máquina virtual a un servidor físico (párr. 4 - 5).

Tanto la computación en la nube como la virtualización han permitido a las compañías ampliar sus operaciones y transacciones en un mercado totalmente tecnológico. Así como muchas organizaciones, PRICOSE, Primera Sociedad Agencia de Seguros S.A, tiene como enfoque, seguir posicionándose en dicho mercado, como una de las primeras agencias de seguros a nivel nacional; esto lo ha logrado por el esfuerzo de inversión en aspectos tecnológicos, pues lo ve como una necesidad estratégica para el alcance de sus objetivos y metas. Es por lo anterior, que PRICOSE ha transformado su negocio hacia la computación en la nube, con servicios automatizados, máquinas virtualizadas y sistemas al alcance del que lo necesite, con solo tener acceso a internet, esto por medio de la plataforma de servicios de Azure de la empresa Microsoft.

En este sentido, Microsoft (s. f.), comenta sobre Azure:

> La plataforma Azure está compuesta por más de 200 productos y servicios en la nube diseñados para ayudarle a dar vida a nuevas soluciones que permitan resolver las dificultades actuales y crear el futuro. Cree, ejecute y administre aplicaciones en varias nubes, en el entorno local y en el perímetro, con las herramientas y los marcos que prefiera. (párr. 1).

Según Conzultek (s. f), Microsoft Azure tiene una amplia clasificación sobre los diferentes servicios ofrecidos, en donde las empresas pueden analizar cuáles de estos son los requeridos, según sus necesidades y los objetivos que se persigan; dentro de los servicios que se pueden mencionar:

Web y móvil: creación de desarrollo, la expansión de aplicaciones web y por medio de los móviles, sumando a la generación de informes, servicios de administración del desarrollo y de notificaciones.

Analítica: permiten controlar los datos en tiempo real para tener una percepción clara de la(s) situación(es) que están ocurriendo en un momento determinado, analizando de esta forma ya sean datos pequeños o una *big data*.

Cómputo: recursos como lo son las máquinas virtuales tanto para Linux como para Microsoft, acceso aplicaciones remotas y contenedores.

Provisión de datos: por medio de los servicios de SQL y NoSQL al igual que mediante el almacenamiento en la nube y en el caché que manejan.

Redes: todo lo que conlleva a conexiones, se tiene acceso a la gestión del tráfico para manejar adecuadamente el rendimiento de los servicios, así como la moderación de las cargas y la opción de hospedaje del sistema de DNS (sistema de nombre de dominios).

Gestión y seguridad: se logra disponer y ejecutar trabajos por medio de la implementación del Azure y tiene la cabida para identificar las amenazas que se presentan y de esta forma atenderlas en un tiempo óptimo.

Administración de identidades y accesos: estos servicios son brindados por Azure para que los usuarios que tengan acceso a los recursos de la plataforma sean los que realmente se encuentren autorizados, ayudando a proteger la información confidencial por medio de contraseñas cifradas.

Debido a todos los cambios que generan las nuevas tecnologías, por parte de las organizaciones, se mantiene una incertidumbre sobre el uso de la nube, por el temor a la pérdida de información, aspectos de ciberseguridad de la infraestructura de TI y ante el manejo y control de los datos, lo anterior tiende a provocar desconfianza entre el suscriptor del servicio en la nube (cliente) y el proveedor de servicio, por lo que, con el cumplimiento de estándares de seguridad, se llega a estrechar esa relación entre cliente – proveedor. Farrall (2020) quien es CISO (Chief Information Security Officer) en la empresa Skytap, hace referencia a las responsabilidades entre proveedores y clientes de los servicios en la nube:

> En términos generales, los proveedores de infraestructura son responsables de proteger la propia infraestructura, incluidas las personas, el hardware, el software, las redes y las instalaciones físicas que componen la plataforma de alojamiento. Los clientes suelen ser responsables de proteger sus propios entornos, incluido el sistema operativo invitado, las aplicaciones y los datos.
> Es esencial que los clientes sepan dónde comienza su responsabilidad y dónde termina el proveedor de infraestructura para evitar cualquier brecha que pueda convertirse en vulnerabilidades (párr. 6).

La seguridad de la información que las organizaciones hospedan en la nube tiene que estar encaminada a un cumplimiento proactivo hacia la detección de cualquier tipo de vulnerabilidad en los ambientes de TI, además de estar dirigidas a un análisis realizado de manera frecuente, en donde se logre medir los procesos que realiza cada empresa; en este sentido, se entiende que la seguridad de los datos, más allá de una inversión a corto, mediano o largo plazo, se volvió en una necesidad que debe enfrentarse lo más eficiente y eficaz posible.

CAPÍTULO III: MARCO METODOLÓGICO

En el presente apartado, se definen los aspectos metodológicos que se utilizarán para realizar la selección de los datos con el fin de generar un análisis y obtener los resultados para construir el diseño de la propuesta. Con respecto al marco metodológico, Mata (2019) comenta:

> El marco metodológico es una elaboración compleja que agrupa las decisiones teórico-metodológicas del proceso investigativo.
>
> Efectivamente, entendido como estrategia teórico-metodológica, el marco metodológico ocupa un papel central respecto a la interrelación que vincula a todas las etapas del proceso investigativo en su conjunto (párr. 6-7).

Enfoques de la investigación

El enfoque de la investigación busca alcanzar los objetivos propuestos en un proyecto por lo que se convierte en una base fundamental para la comprensión y desarrollo de todas las etapas del proceso.

Enfoque cuantitativo.

En este enfoque se pretende una investigación con la mayor objetividad posible, se debe realizar una recolección de datos para luego llevarlos al análisis y de esta forma comprobar la hipótesis establecida. Dicho enfoque debe ser medible por lo cual, por medio de una muestra realizada a una población en específico, se deberán generar los resultados. Fernández, Baptista y Hernández (2014) se refieren al término de investigación cuantitativa:

> La investigación cuantitativa ofrece la posibilidad de generalizar los resultados más ampliamente, otorga control sobre los fenómenos, así como un punto de vista basado en conteos y magnitudes. También, brinda una gran posibilidad de repetición y se centra en puntos específicos de tales fenómenos, además de que facilita la comparación entre estudios similares (p. 15).

Enfoque cualitativo.

Con respecto al enfoque cualitativo, Fernández, Baptista y Hernández (2014) mencionan que “la investigación cualitativa proporciona profundidad a los datos, dispersión, riqueza interpretativa, contextualización del ambiente o entorno, detalles y

experiencias únicas. Asimismo, aporta un punto de vista “fresco, natural y holístico” de los fenómenos, así como flexibilidad” (p. 16).

La orientación de este enfoque se va estructurando de acuerdo con los eventos que van ocurriendo y conforme a la ejecución del estudio. Un punto importante de este enfoque es que la revisión inicial puede ser perfeccionada en cualquier etapa del estudio. Influye la lógica y el razonamiento, por lo cual la investigación se va efectuando entre la experiencia de lo investigado, la acción por seguir y los resultados. Dentro de las técnicas que se pueden aplicar están la observación, la revisión de documentos oficiales, los cuestionarios, entre otros.

Enfoque mixto.

Al respecto, Fernández, Baptista y Hernández (2014) citando a Hernández y Mendoza (2008) comentan que:

> …los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (metainferencias) y lograr un mayor entendimiento del fenómeno bajo estudio” (p.17).

En este enfoque se toman de base tanto el enfoque cuantitativo como el cualitativo, no se trata de reemplazar a ninguno, más bien, se toman las fortalezas de ambos para integrarlos a la investigación.

En la figura N°3 se ilustran los tres tipos de enfoques de la información, con características específicas tanto del cualitativo como del cuantitativo y como el centro de ellos, el mixto, en donde se demuestra que es la suma de la combinación de los ya mencionados.

Figura 3. Enfoques de la investigación.

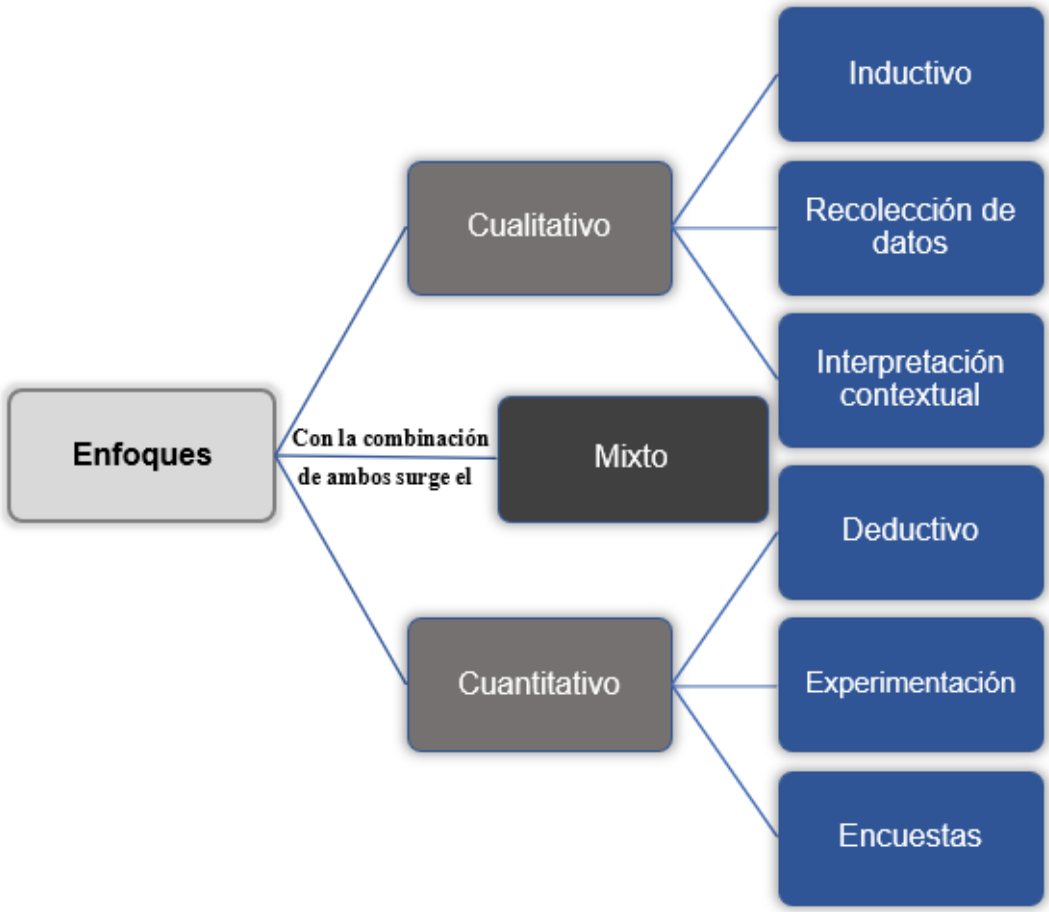

Figura 3. Enfoques de la investigación.
Elaboración propia.

Enfoque de investigación seleccionado.

Luego de analizado cada uno de los enfoques de investigación, el desarrollo de este proyecto se hará bajo el enfoque mixto, por cuanto se elaborarán encuestas donde se logre medir y demostrar el grado de conocimiento que los empleados de la empresa tienen sobre la seguridad de los datos alojados en la nube; a su vez, se deberán aplicar técnicas de observación, estudio de riesgos y amenazas presentes en la compañía, para que, con la integración de la información brindada y recolectada, se puedan realizar propuestas de mejoras hacia la seguridad de los datos; además, se estudiarán las normas de seguridad, con el fin de determinar el cumplimiento de los procedimientos descritos por la ISO 27017.

Métodos de la investigación

Así como es importante el enfoque que se utiliza para efectuar un estudio, también es necesario saber el tipo de investigación que se aplicará, según el propósito del proyecto y los medios manejados para obtener los resultados esperados. Abreu (2014) se refiere al método de la investigación:

> El método de la investigación describe con buenos detalles la forma en que se ha llevado a cabo la investigación. Este permite explicar la propiedad de los métodos utilizados y la validez de los resultados, incluyendo la información pertinente para entender y demostrar la capacidad de replicación de los resultados de la investigación. (p. 195).

Método descriptivo.

Reside en describir los datos y características de la población en estudio. Se basa en la observación, se pretende conocer los escenarios mediante las actividades, procesos o personas. Explica cómo es esa parte de la realidad del objeto en estudio; se deben recolectar los datos, se analizan de una forma muy cuidadosa y luego se exponen los resultados. Al respecto de la investigación descriptiva (Abreu, 2012) menciona:

> La investigación descriptiva encaja en las dos definiciones de las metodologías de investigación, cuantitativas y cualitativas, incluso dentro del mismo estudio. La investigación descriptiva se refiere al tipo de pregunta de investigación, diseño y análisis de datos que se aplica a un tema determinado. La estadística descriptiva responde a las preguntas quien, que, cuando, donde y como[sic] (p. 192).

Método analítico.

Este método consiste en fragmentar un todo en elementos para observarlos y determinar las causas y efectos. Abreu (2014) amplía el concepto de la siguiente forma:

> Se fundamenta en la premisa de que a partir del todo absoluto se puede conocer y explicar las características de cada una de sus partes y de las relaciones entre ellas.

> El método analítico permite aplicar posteriormente el método comparativo, permitiendo establecer las principales relaciones de causalidad que existen entre las variables o factores de la realidad estudiada. Es un método fundamental para toda investigación científica o académica y es necesario para realizar operaciones teóricas como son la conceptualización y la clasificación (p. 199).

Método comparativo.

La técnica comparativa consiste en establecer una comparación de los elementos que se están estudiando y ello es aprovechado para la comprobación de hipótesis. Abreu (2014) lo describe:

> Este método consiste en establecer analogías y disimiludes [sic] con enfoques de búsqueda diferenciadora y búsqueda antagónica. El método comparativo ayuda a establecer distinciones entre sucesos o variables que son repetitivos en realidades estudiadas, esto conlleva en algunos casos a una característica de generalidad y en otros casos a la particularidad (p. 199).

Método inductivo.

Este método está apoyado en el razonamiento, en donde admite saltar de los hechos particulares, por medio de estudios u observaciones para generar conclusiones con fundamentos más generales. Así lo ejemplifica Abreu (2014):

> El método inductivo plantea un razonamiento ascendente que fluye de lo particular o individual hasta lo general. Se razona que la premisa inductiva es una reflexión enfocada en el fin. Puede observarse que la inducción es un resultado lógico y metodológico de la aplicación del método comparativo.

Tipo de investigación seleccionado.

Luego de analizados los métodos de investigación descritos, el proyecto se orientará bajo la investigación descriptiva, se almacenarán los datos y se organizarán para luego de ello, analizar los resultados de las observaciones y estudios encontrados, para manifestar la percepción clara de las situaciones específicas que se descubran.

PRICOSE carece de requerimientos en cuanto a la seguridad de la información en la nube y aunado a ello, se requiere de un profundo análisis de los controles. En esta investigación se describirán las normas propuestas por la ISO 27017 para estudiar sus controles y adecuarlas a la situación actual en la empresa.

Fuentes de información

Las fuentes que se utilizan para describir el inicio de una información específica sobre la que es desarrollada la investigación, es el principal apoyo en el que se fundamenta el estudio. Una de las razones del porqué es necesario apoyarse en las fuentes de información, es la de generar datos lo más fehacientes posibles. Refiriéndose al término, García (2019) comenta:

> Las fuentes de información son instrumentos para el conocimiento, acceso y búsqueda de la información, su objetivo principal es el de buscar, fijar y difundir la fuente de información implícita en cualquier soporte físico, estas se pueden catalogar desde diferentes perspectivas, sin embargo, cada autor puede elaborar su propia clasificación dependiendo su grado de información. De acuerdo con el grado de información que proporcionan, las fuentes de información se dividen en primarias, secundarias y terciarias; esta división se utiliza generalmente en el ámbito académico (pág. 57).

Las fuentes de información están compuestas por tres grupos:

Fuentes primarias.

Son las que dominan la información original, como ejemplo se pueden mencionar las revistas científicas, documentación oficial, tesis, la persona entrevistada, entre otros.

Según la Universidad del Sur de California (2021):

> Las fuentes primarias son materiales que fueron creados durante el período de tiempo que se está estudiando o que fueron creados en una fecha posterior por un participante en los eventos que se están estudiando, como una memoria de la infancia. Son documentos originales [es decir, no se trata de otro documento o

> cuenta] y reflejan el punto de vista individual de un participante u observador. Las fuentes primarias representan registros directos y no interpretados del tema de su estudio de investigación (párr. 1).

Fuentes secundarias.

El contenido de dicha información proviene de un producto de extracciones, reorganizaciones y análisis que son resultantes de las fuentes primarias, se puede hablar de las biografías, artículos de revista o internet.

La revisión de material de fuente secundaria puede ser valiosa para mejorar su trabajo de investigación en general porque las fuentes secundarias facilitan la comunicación de lo que se sabe sobre un tema (Universidad del Sur de California, 2021).

Fuentes terciarias.

Son una sucesión de guías tanto físicas como virtuales sobre lo que son las fuentes secundarias, ejemplos de ellos son los directorios y artículos sobre encuestas.

Al respecto, La Universidad del Sur de California (2021) hace referencia a que las fuentes terciarias son buenos puntos de partida para proyectos de investigación porque a menudo extraen el significado esencial o los aspectos más importantes de grandes cantidades de información en un formato conveniente.

Fuentes de información seleccionadas.

En la investigación se utilizarán las fuentes primarias, mediante una encuesta que se les aplicará a los empleados de la aseguradora PRICOSE. Para el caso de las fuentes secundarias, como la principal se tomará la ISO 27017 y el apoyo de la ISO 27002, adicionalmente, los libros digitales sobre la seguridad de la información. Por último, en cuanto a las fuentes terciarias, se consultarán referencias bibliográficas, con el fin de sustentar la información desarrollada en el estudio.

Variables de investigación

Las variables son utilizadas para medirlas, observarlas y analizarlas mientras se realiza el proceso de la investigación. Hernández (2017) ilustra que la definición de variable es:

> Una variable es una propiedad o característica de fenómenos, entidades físicas, hechos, personas u otros seres vivos que puede fluctuar y cuya variación es susceptible de medirse u observarse. (pág. 82). Las variables son agrupadas de tres formas:

Variables conceptuales.

Las variables conceptuales hacen referencia a la definición técnica de lo que se quiere dar a entender, respaldada de una fuente de expertos mediante citas textuales. Hernández (2017) conceptualiza el término de la siguiente forma:

> La definición conceptual o constitutiva es la acordada y validada por una comunidad científica o profesional. Generalmente estas definiciones se encuentran en diccionarios especializados, páginas electrónicas con respaldo institucional y publicaciones (como artículos de revistas académicas y libros) (pág. 87).

Variables operacionales.

Las variables operacionales es el proceso en donde, se crean las instrucciones prácticas que admiten la elaboración de los datos reales para validar la hipótesis y de esta forma, corregir las dificultades. De igual forma, Hernández (2017) comenta de las variables operacionales:

> Especifica qué actividades u operaciones deben realizarse para medir una variable. La definición operacional nos dice que, para recoger datos respecto de una variable, hay que hacer esto y esto otro. Además, articula los procesos de un concepto que son necesarios para identificar sus ejemplos.

Variables instrumentales.

Son las que definen la manera en que se experimentará la variable que se concretó, los instrumentos o medios que se utilizaran para la recolección de los datos. Moreno (2013) comenta al respecto:

> En este ítem se aclara como se estudiará la variable que se acaba de definir, los medios o instrumentos para recoger la información. En mérito de ello se deben definirse y elaborarse los instrumentos y medios con que se recolectará la

información. Los instrumentos nacen de las variables y de los objetivos. Nunca deberá elaborarse un instrumento sin tener definida la variable o variables. (párr. 10).

En la tabla N°1 se observa el análisis de los tres grupos de variables, tomando de base principal los objetivos específicos indicados en el apartado de objetivos.

Tabla 1. Análisis de las variables.

Análisis de las variables				
Objetivo Específico	**Variable**	**Variable conceptual**	**Variable operacional**	**Variable instrumental**
Concienciar al personal de TI sobre las normas de seguridad para la información alojada en la nube.	Concienciación sobre la seguridad de la información	Según Gaviria (s. f) la concienciación de la seguridad "Se trata de un conjunto de medidas que una organización toma para proteger la confidencialidad, integridad y disponibilidad de la información sensible, y se constituyen en un elemento esencial del programa de seguridad de información de cualquier empresa.".	Generar una encuesta para determinar el grado de conocimiento sobre la seguridad de la información y luego de ello, desarrollar un plan de capacitación sobre aspectos básicos y esenciales de la seguridad de la información.	Diseño de la encuesta. Diseño del plan de capacitación.
Identificar las amenazas de acceso, divulgación o modificación de información que se presentan en la organización basado en la norma ISO 27017.	Amenazas de acceso a la información.	Una amenaza según Tarazona (s. f), "en términos simples es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan." (pág. 137-138).	Reuniones con el encargado del departamento de TI. Revisión de la plataforma Microsoft Azure.	Documento de diseño de la entrevista. Documento de diseño de la observación.

Tabla 1. Análisis de variables.

Elaboración propia (2021)

Tabla 2. Análisis de las variables.

Análisis de las variables				
Objetivo Específico	**Variable**	**Variable conceptual**	**Variable operacional**	**Variable instrumental**
Clasificar la información de acuerdo con su orden de sensibilidad según la norma ISO 27017.	Clasificación de la información.	Según la Escuela Europea de Excelencia (2019): "La clasificación de la información según ISO 27001 es un proceso en el que la organización evalúa los datos que posee y el nivel de protección que cada uno requiere. Se trata de uno de los aspectos más complejos, pero sin duda más interesantes, en la gestión de la seguridad de la información."	Reuniones con el departamento de TI para inventariar la información y luego de ello clasificarla de acuerdo con su nivel de prioridad. Revisión de la plataforma Microsoft Azure.	Documento de guía de observación. Documento del inventario de la información.
Establecer políticas sobre el uso que se le da a la información y la forma en que será compartida basado en la norma ISO 27017.	Políticas de seguridad.	Las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad integridad y disponibilidad de la información y minimizar los riesgos que le afectan (Universidad Internacional de La Rioja, 2020).	Elaboración de las normas para la seguridad de la información. Revisión de la Norma ISO 27017.	Documento de diseño de las políticas de seguridad.
Formar los roles y responsabilidades internas en la compañía, con respecto a la seguridad de la información hospedada en la nube.	Roles	Según ITIL V3, "un rol es un conjunto de actividades y responsabilidades asignada a una persona o un grupo. Una persona o grupo puede desempeñar simultáneamente más de un rol" (Universidad Politécnica de Valencia, s. f).	Entrevista con el encargado de TI para la identificar roles presentes en el área. Revisión de la norma ISO 27017	Documento de diseño de entrevista. Documento de la norma ISO 27017

Tabla 2. Análisis de las variables.

Elaboración propia (2021)

Población de la investigación.

La población es el conjunto de los individuos, fenómenos u objetos estudiados, relacionado con el tema en desarrollo, en procura del logro de los objetivos propuestos.

Con respecto al término de población y según López (2004):

> Es el conjunto de personas u objetos de los que se desea conocer algo en una investigación. "El universo o población puede estar constituido por personas, animales, registros médicos, los nacimientos, las muestras de laboratorio, los accidentes viales entre otros". (PINEDA et al 1994:108) En nuestro campo pueden ser artículos de prensa, editoriales, películas, videos, novelas, series de televisión, programas radiales y por supuesto personas (pág. 69).

El estudio se llevará a cabo en la empresa PRICOSE, ubicada en la provincia de Goicoechea, con un total de 136 agentes de seguros y 34 colaboradores, se trabajará con la ayuda de dicha población, para obtener datos relevantes que apoyen el progreso de la propuesta.

Muestra de la investigación.

La muestra de la investigación es una parte de la cantidad de la población estudiada, se toma de referencia el subgrupo en donde se pueda obtener la información de interés para que ilustre de manera representativa, los resultados esperados.

Al respecto, Hernández (2014) hace referencia al término de muestra:

> Muestra (es un subgrupo de la población o universo). Se utiliza por economía de tiempo y recursos. Implica definir la unidad de muestreo y de análisis. Requiere delimitar la población para generalizar resultados y establecer parámetros (pág. 171).

La fórmula más común para la aplicación de la muestra en esta investigación es mediante una población finita ya que se conoce la cantidad de fenómenos, personas u objetos a observar, Según Aguilar (2005), la muestra es ejecutada mediante la siguiente operación:

Figura 4. Fórmula de muestra de la investigación.

$$n = \frac{N Z^2 \quad pq}{d^2 \ (N - 1) + Z^2 \quad pq}$$

Figura 4. Fórmula de muestra de la investigación.

En donde:

n representa el tamaño de la muestra.

N se refiere al tamaño de la población.

Z es el valor crítico, llamado también como nivel de confianza.

p representa la proporción esperada del fenómeno que se está estudiando.

q es la proporción de la población que no representa el fenómeno en estudio, también llamado como la probabilidad de fracaso.

d referido al nivel de precisión absoluta (margen de error).

Si se desconoce el nivel confianza (Z), es un valor contante, se toma en relación con el 95% de confianza, equivalente a 1,96 (la medida más recomendable de utilizar). El porcentaje de riesgo máximo que se recomienda correr es de un 5% (normal para las ciencias sociales). La cantidad de fenómenos de la población (p), tiene una relación con la variable que se requiere medir, el número de personas o fenómeno que no participan en esa variable se marca con (q). Para las dos medidas se colocará un 0,5.

Para dicha investigación, los individuos que se utilizarán para comprobar la muestra serán los empleados internos que se encuentran en la oficina central de PRICOSE, de ser así, se tomará de base una cantidad de 34 individuos, de tal manera, la formula quedará así:

N = 34 Z = 1,96 d = 0,05 p y q = 0,5

n= 34 x 1,96 ² x 0,5 x 0,5 / 0,05 ² (34 – 1) + 1,96 ² x 0,5 x 0,5

n= 32,6536 / 0,05 ² x 33 + 1,96 ² x 0,5 x 0,5

n= 32,6536 / 0,0825+ 1,96 ² x 0,5 x 0,5

n= 32,6536 / 0,0825 + 0,9604

n= 32,6536 / 1,0429

n= 31, 31

En el estudio de la fórmula anterior, se busca la muestra más acorde para el desarrollo del proyecto, con un nivel de confianza de un 95% y una probabilidad de error del 0,05; el resultado proyecta que la muestra debe ser de 31 empleados de la organización.

Instrumentos de recolección de datos

Los instrumentos para la recolección de datos son los recursos de los que los investigadores pueden valerse para aproximarse a los objetos o personas y así recaudar la información deseada y necesaria. El o los instrumentos por utilizar, dependerá del tipo de investigación que se esté desenvolviendo, por lo cual puede ser necesaria la aplicación de uno a más instrumentos para la obtención de la información.

En este sentido, Mendoza y Ávila (2020) afirman:

> Las técnicas de recolección de datos comprenden procedimientos y actividades que le permiten al investigador obtener información necesaria para dar respuesta a su pregunta de investigación. Existen múltiples y diferentes instrumentos útiles para la recolección de datos y para ser usados en todo tipo de investigaciones ya sean cuantitativas, cualitativas o mixtas (pág. 52).

La recolección de datos en un estudio proviene de la utilización de una serie de mecanismos o instrumentos que generan un soporte esencial al momento del análisis de los resultados, con lo cual se reúne información de manera organizada.

Dentro de los instrumentos, se mencionarán los que se van a utilizar en este trabajo:

Encuesta.

Se clasifican dentro de las técnicas más utilizadas para la obtención de datos importantes acerca de un tema específico o de personas u objetos para lograr compararlos, describirlos o explicar su comportamiento. Se diseñan mediante un listado de preguntas, recomendablemente, con preguntas cerradas, donde se tenga una respuesta precisa y un análisis en un menor tiempo posible y pueden ser adecuadas a todo tipo de población y de información.

Al respecto, Torres (2019) se refiere al término de encuesta de la siguiente manera:

> Constituye el término medio entre la observación y la experimentación. En ella se pueden registrar situaciones que pueden ser observadas y en ausencia de poder recrear un experimento se cuestiona a la persona participante sobre ello. Por ello, se dice que la encuesta es un método descriptivo con el que se pueden detectar ideas, necesidades, preferencias, hábitos de uso, etc. (p. 4).

Para esta investigación, el método de encuesta permitirá tener datos de una cantidad de empleados, con ello se agiliza el proceso sin tener que estar presente, ya que se enviará por algún medio masivo como es el correo electrónico, luego, se evaluará el conocimiento que tiene cada empleado sobre los controles de seguridad de la información que la empresa resguarda en la nube.

Entrevista.

La entrevista es la herramienta de intercomunicación personal que se da entre el investigador y el objeto de estudio, con el fin de conseguir respuestas ante el problema planteado. Torres (2019) afirma que este es el instrumento de mayor importancia en la exploración, junto con el cuestionario; con ella se logran resultados subjetivos del encuestado con respecto a las preguntas del cuestionario.

El método de la entrevista será ejecutado con la persona encargada del departamento de TI, el fin es tener una percepción del conocimiento que se posee acerca de las normas de seguridad de los datos en la nube, así como validar cuáles son los controles de la empresa sobre las responsabilidades entre su proveedor y como clientes.

Observación.

Método que justamente radica en observar el desarrollo de la persona, fenómeno y objeto, que se pretende analizar. Puede ser utilizada para datos tanto cuantitativos como cualitativos, dependiendo la forma en que se ejecute. Se deben determinar los datos por observar y registrar la información de forma ordenada. Según Orellana (2006):

> Las técnicas de recolección de datos basadas en la observación y participación, practicadas en entornos convencionales, consisten en la observación que realiza el investigador de la situación social en estudio, procurando para ello un análisis de forma directa, entera y en el momento en que dicha situación se lleva a cabo,

y en donde su participación varía según el propósito y el diseño de investigación previstos (p. 211).

Se utilizará el método de observación de la información configurada en los servicios de la nube, en la plataforma Microsoft Azure; con ello, se logrará identificar las amenazas presentes en la organización, se clasificarán los datos, según la prioridad y sensibilidad que se merezca y se establecerán los roles adecuados para el lineamiento de las responsabilidades individuales como las compartidas entre el proveedor de servicio en la nube y la compañía.

Proceso para la recolección y análisis de datos

Para el desarrollo de la investigación y obtener los resultados del estudio, se tomarán de apoyo tres de los instrumentos de recolección de datos: la encuesta, la entrevista y el método de observación.

En el caso de la encuesta, se realizará una serie de preguntas, según el apéndice 1, dirigidas a una muestra del personal interno de PRICOSE. La idea es que los tipos de preguntas por desarrollar sean cerradas, para que se refleje el conocimiento del personal ante la seguridad de la información y del manejo de los activos de la organización. La encuesta será ejecutada mediante la herramienta gratuita de Google *Forms*, debido a que la empresa la utiliza cuando realizan encuestas, por lo cual al personal le resultará familiar y de fácil uso.

En el caso de la entrevista referido al apéndice 2, se le aplicará a una persona específica, quien es el encargado del departamento de tecnologías de la información. Se pretende identificar los procesos que se realizan para proteger los datos alojados tanto en la nube privada como en la pública. Además de validar la existencia de controles para mantener una adecuada gestión en cuanto al manejo de la información. Para la obtención de los resultados de la entrevista, se elaborará una serie de preguntas como estilo cuestionario, en donde se manejará, por medio de una conversación directa y de manera informal.

Por último, el método de observación en el apéndice 3, se realizará de una forma directa, desde la plataforma de Microsoft Azure, se tomará como sujeto de estudio la configuración de dicha herramienta. En compañía del encargado de TI, se revisarán todas aquellas tareas automatizadas, se identificarán los activos presentes en su nube pública y privada, se analizarán los controles de seguridad de la plataforma y el funcionamiento que se les da a estos. La observación, se realizará en un lapso determinado, llevando diariamente una bitácora, donde se expondrán las tareas realizadas por día y los resultados logrados.

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

En el presente capítulo, se expone la forma en que fueron ejecutados los instrumentos de recolección de la información para obtener los resultados necesarios que brinden un análisis sobre la situación de la empresa; en este caso, la forma en que se maneja la seguridad de la información alojada en la nube.

Interpretación de los resultados de la encuesta

Para el caso de la encuesta según el anexo 1, se realizó un listado de 15 preguntas cerradas, de tipo selección única; para su aplicación, se tomó a 31 empleados que corresponden a la cantidad total de la muestra.

El fin de la encuesta es que, por medio de preguntas generales sobre la seguridad de la información que cada uno maneja, se demostrará el grado de conocimiento y con ello, se logran los objetivos específicos de concienciar al personal, establecer políticas sobre el uso que se le da a la información y la formación de roles dentro de la compañía. Posteriormente, se ejemplificará el cuestionario ejecutado, con las respuestas globales, su diseño gráfico porcentual y se finaliza con su interpretación.

Grado de conocimiento sobre la seguridad de la información.

De acuerdo con los resultados obtenidos, se pretende concienciar al personal sobre el uso adecuado que se le debe dar a la información, manteniendo en todo momento la seguridad adecuada.

Gráfico 1. Seguridad de la información

Gráfico 1. Conocimiento de la seguridad de la información.
Fuente: elaboración propia.

En relación con las respuestas del gráfico 1, se observa que un 83,9% afirma conocer el término general de seguridad de la información, el 12,9% no está seguro de conocerlo y el 3,2% indica que, en definitiva, no conoce lo que es la seguridad de la información. El 83,9% representa un total de 26 sobre 31 empleados, por lo que se deduce que el personal comprende la importancia que tiene la seguridad sobre la información.

Gráfico 2. Identificación de amenazas

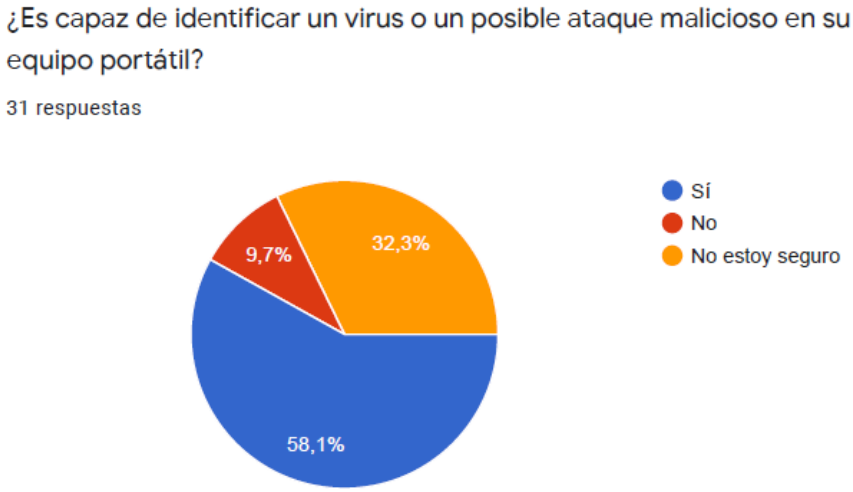

Gráfico 2. Identificación de amenazas.
Fuente: Elaboración propia.

Para este caso, en el gráfico 2, se intenta conocer si los empleados logran identificar una amenaza en sus equipos, se obtuvo un 58,1%, que se siente capaz de reconocer una potencial amenaza, un 32,3% se muestra inseguro y el 9,7% reconoció no saber en qué momento recibe una sospecha de virus o amenaza en sus equipos de trabajo. Resumiendo, el 41,9% para una cantidad de 13 personas, pueden estar recibiendo un virus, ya sea por medio de su correo electrónico, por medio de su WhatsApp empresarial, o bien, mediante un compartido en la nube y ante el desconocimiento de que dicho documento sea sospechoso, existe una posibilidad de que cada una de estas personas pueda abrir e infectar a todos los demás equipos ligados a la red.

Gráfico 3. Riesgos en redes wifi

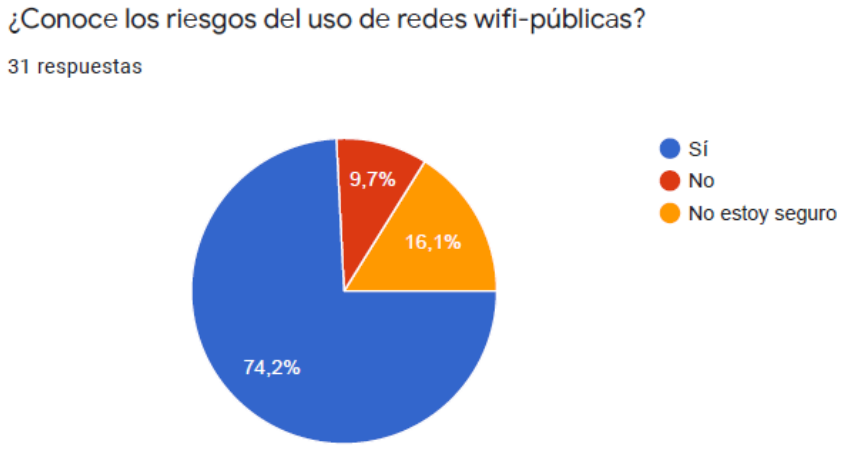

Gráfico 3. Riesgos en redes wifi.
Fuente: Elaboración propia.

En el gráfico 3, se pretende reconocer si los empleados están conscientes de los riesgos que pueden implicar el conectarse a redes wifi-públicas, más sabiendo que todos se encuentran realizando teletrabajo, por lo que el internet requerido es consumido desde sus redes de hogares. Se registró un 74,2% de personas que tiene conocimiento sobre las redes utilizadas en este momento, un 16,1% se muestra inseguro de conocer estos riesgos y el 9,7% niega conocer los riesgos que esta conexión puede traerle si no se manejan de una forma adecuada. Se suman las personas que no están seguras con las que, en efecto no conocen los riesgos, se recuenta un 25,8% equivalente a 8 personas del total de la muestra.

Gráfico 4. Prevención de riesgos

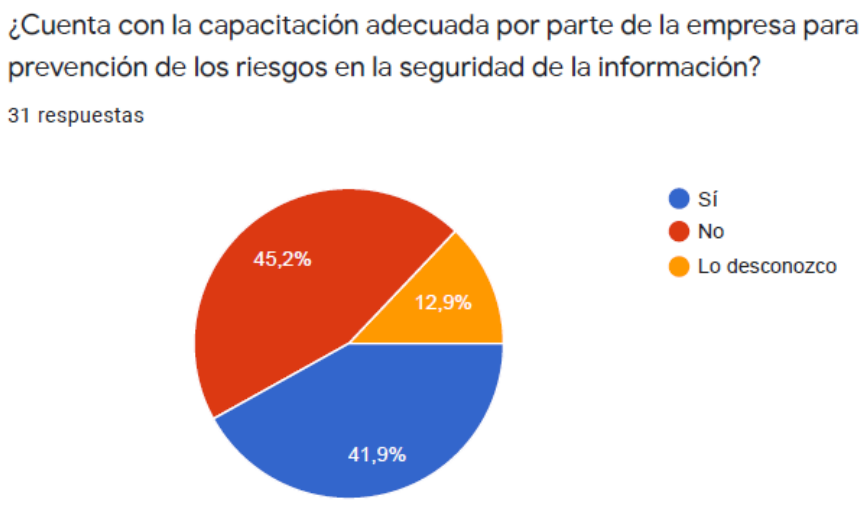

Gráfico 4. Prevención de riesgos.
Fuente: Elaboración propia.

En el gráfico 4 se muestra el resultado de la interrogación referida a si la empresa ofrece alguna formación de cómo se logran prevenir los riesgos que pueden surgir ante una mala gestión de la seguridad sobre la información que se maneja en la organización; para ello, un 41,9 % indica que sí recibe ese tipo de capacitación, caso contrario un 45,2% expuso que no lo recibe y un 12,9% desconoce si se reciben dichas formaciones. Se logra deducir que un 54,8%, representado por 18 personas sobre el total de la muestra, no han recibo capacitación o preparación en pro de la seguridad de la información.

Identificación de amenazas de acceso.

Con este apartado se pretende reconocer aquellos usuarios que no tienen una seguridad óptima para el ingreso a los sistemas y cuentas de correos que se manejan en la organización.

Gráfico 5. Acceso a los sistemas

Gráfico 5. Acceso a los sistemas.
Fuente: Elaboración propia.

Con respecto al gráfico 5, se demuestra que el 90,3% de los empleados encuestados, cuenta con un usuario y contraseña única para el acceso a los diversos sistemas que utiliza; el 6,5% indica que no posee un usuario y contraseña, mientras que el 3,2% desconoce si tiene esa seguridad para dicho ingreso.

Gráfico 6. Doble factor de autenticación

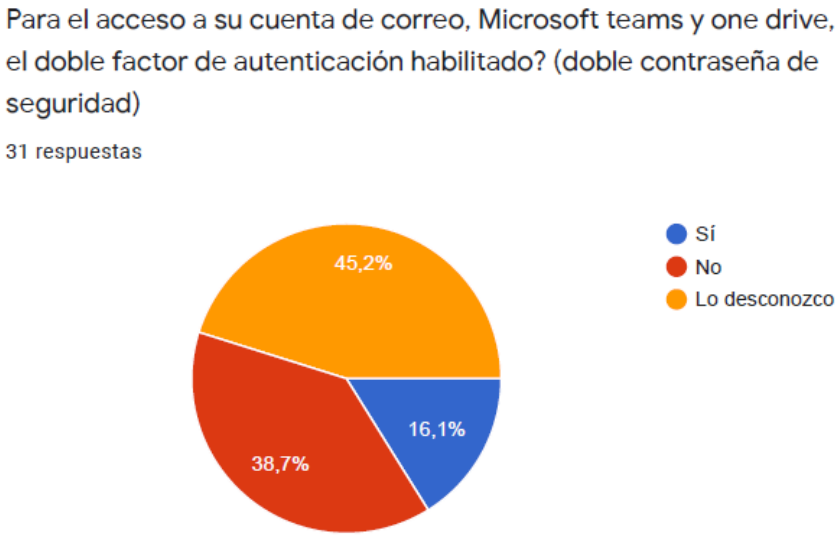

Gráfico 6. Doble factor de autenticación.
Fuente: Elaboración propia.

Con el gráfico 6, se evalúa si la seguridad de doble factor de autenticación se encuentra habilitada en todas las cuentas empresariales de Office 365 que tiene la compañía. Se detecta que un 38,7% no tiene la doble seguridad habilitada, el 45,2% desconoce si se mantiene la opción habilitada y solamente el 16,1% que representa a 5 personas del total de la muestra, indica tener la doble autenticación para sus accesos.

Gráfico 7. Uso de contraseñas

Gráfico 7. Uso de contraseñas.
Fuente: Elaboración propia.

En el gráfico 7 se muestra el análisis acerca de si los empleados tienen noción del buen o mal uso que hacen con las contraseñas utilizadas y, según esto, el 83,9% siente que hace uso adecuado de las contraseñas, el 3,2% comenta que no utiliza de forma apropiada sus claves, mientras que el 12,9% no está seguro de utilizarlas de forma correcta.

Roles y normas de seguridad.

Para este apartado, se intenta conocer si la compañía cuenta con una clasificación de funciones, las políticas que manejan según los roles y las normas a seguir en cuanto al uso de los activos que utiliza cada empleado.

Gráfico 8. Roles

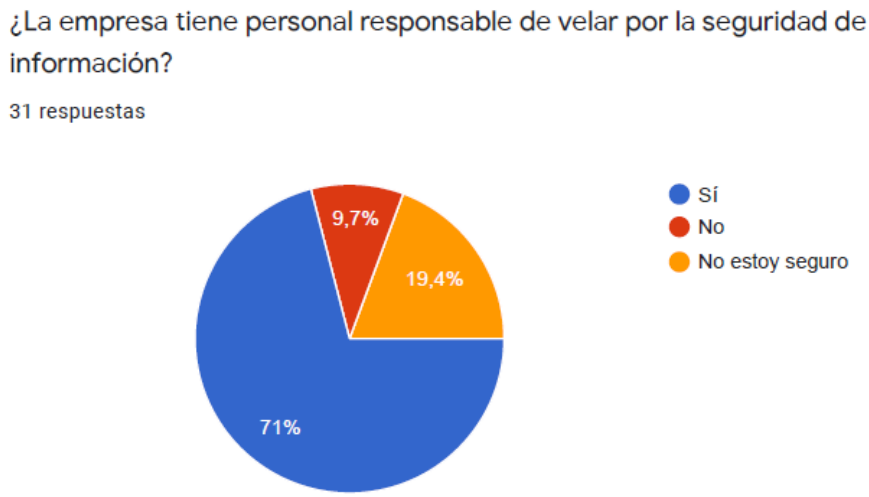

Gráfico 8. Roles de usuarios.
Fuente: Elaboración propia.

El gráfico 8 representa el conocimiento sobre el personal responsable dentro de la organización para velar por la seguridad de la información, el 71% representa el porcentaje de personas que tienen conocimiento de quien vela por la seguridad, el 19,4% desconoce quién o quiénes son los responsables y el 9,7% no está seguro de cuál es el personal que se encarga de dichas funciones.

Gráfico 9. Políticas de funciones

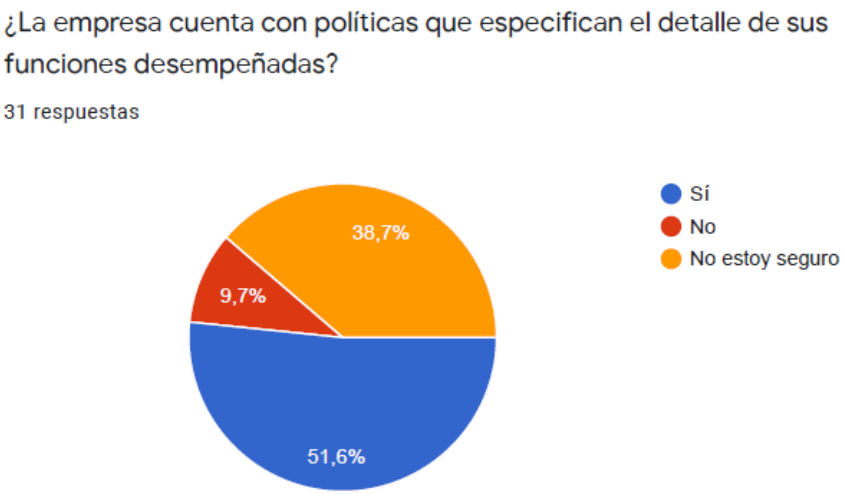

Gráfico 9. Políticas de funciones.
Fuente: Elaboración propia.

El gráfico 9 hace referencia a las políticas de las funciones según el puesto que desempeña cada persona, se refleja que un 51,6% afirma que la organización posee estas políticas de funciones, el 9,7% niega tener alguna norma que especifique el detalle de sus funciones realizada y el 38,7% no está seguro en tener estas políticas. Sumado al 9,7% de negación con el 38,7% que desconoce del tema, se llegaría a un 48,4 representado en 15 empleados del total de la muestra.

Gráfico 10. Normas en el uso de activos

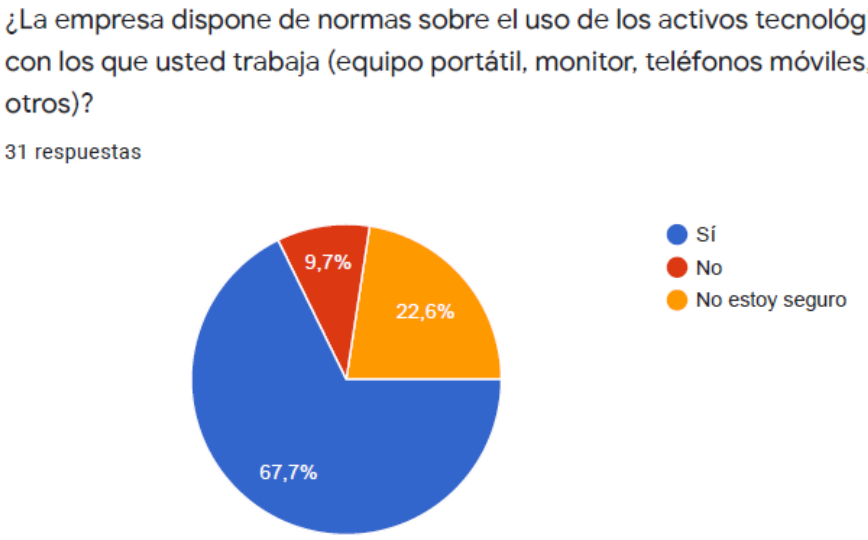

Gráfico 10. Normas en uso de activos.
Fuente: Elaboración propia.

El gráfico 10 hace referencia a las políticas que la organización cuenta para el uso que se les deben dar a los activos tecnológicos, según este, el 67,7% dice contar con estas políticas, el 22,6% desconoce si la empresa tiene este tipo de políticas y el 9,7% niega tener alguna norma que cumpla con la seguridad de los activos. Un total del 32, 3% que representa a 10 empleados encuestados del total de la muestra, parece no contar o no tener claras las normas ante el funcionamiento de sus tareas específicas según el puesto desempeñado.

Gráfico 11. Normas en el uso de datos

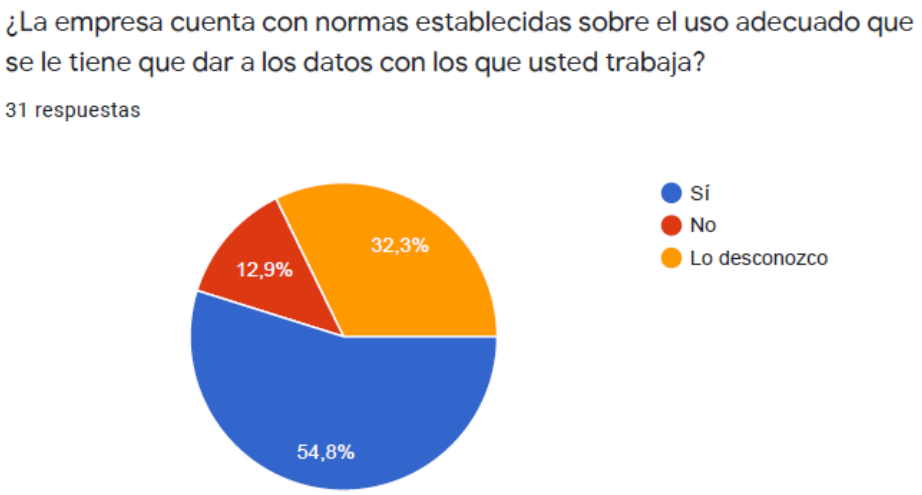

Gráfico 11. Normas en el uso de datos.
Fuente: Elaboración propia.

Con el gráfico 11 se intenta verificar las políticas que la compañía tiene establecidas, con respecto al uso de los datos que cada empleado trabaja, el 54,8% comenta que sí poseen estas políticas, el 12,9% niega tener las políticas y el 32,3% desconoce si tienen o no estas reglas. Un 45,2%, el equivalente a 14 personas del total de la muestra desconoce el tema.

Gráfico 12. Normas en el uso de datos

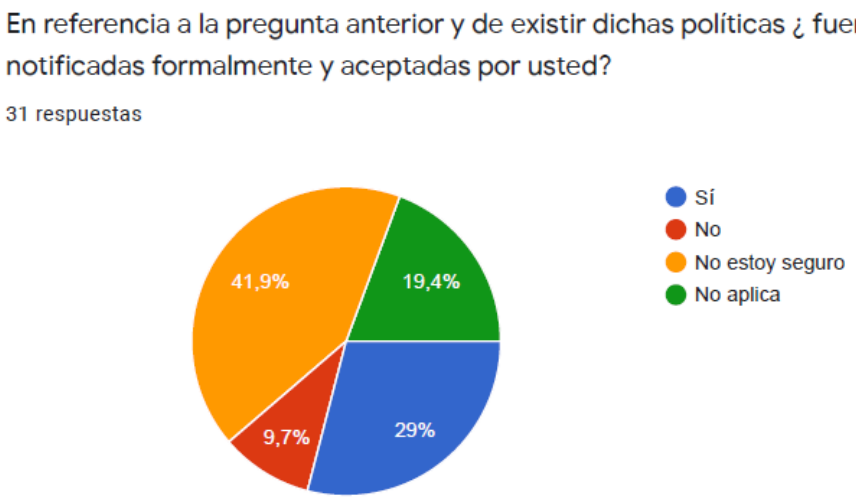

Gráfico 12. Normas en el uso de datos.
Fuente: Elaboración propia.

Con respecto al gráfico 12 en el cual se hace referencia a si las políticas (de ser que existieran) fueron notificadas y aceptadas por cada empleado. Un 29% indica que sí se les comunicó, un 41,9% no está seguro, el 9,7% niega el que les hayan notificado y el 19,4% no ve la pregunta como aplicable. Se muestra que el 71% deja en evidencia no tener realmente claro si existen dichas normas sobre el uso y la importancia de la información con la que trabajan.

Interpretación de los resultados de la entrevista

Se ejecutó una serie de 19 preguntas en la entrevista, el objetivo es tener una percepción de la forma en que resguardan y trabajan la seguridad sobre la información alojada en la nube, en la empresa. La persona entrevistada es el coordinador del área de TI, la entrevista se ejecutó por medio de la plataforma Microsoft *Teams*, formando un diálogo consecuente a las respuestas que el entrevistado iba dando. A continuación, el detalle del análisis luego de finalizado el instrumento:

Plan de prevención de riesgos informáticos.

El entrevistado comenta que la organización sí cuenta con un plan de prevención de riesgos en cuanto a la información, sin embargo, al momento de consultar si podríamos ver el plan de prevención para su análisis, el coordinador comentó que ese tipo de tareas se manejan diariamente por lo cual no cuentan con una documentación

formal o bien, los procedimientos a seguir ante los diferentes riesgos que puedan ocurrir en la compañía.

Controles sobre la información manejada por los usuarios de la organización.

El entrevistado hace mención a que todo lo referente a permisos y accesos a la información brindada a los usuarios, antes de realizar dichos permisos, tiene que venir con la aprobación de los encargados de las diferentes áreas; sin embargo, este tipo de procesos lo hacen de forma, y no tienen una guía o bien línea a seguir para validar que los accesos por departamento sean los mismos entre los usuarios, por ello, se puede deducir, que con el hecho de que la organización no cuente con una guía sobre la clasificación de la información, un usuario de un departamento puede tener mayores privilegios de acceso que otro, cuando en realidad cumplen las mismas funciones. Adicional a ello, hace mención de que no existen normas establecidas en donde se les indique a los usuarios la forma en la cual deban trabajar la información brindada y dejan a la confianza de cada empleado el manejo de esta.

Instrucciones por seguir con diferentes procesos del área de TI.

Adicional a ello, el coordinador hizo una acotación e indicó que no es totalmente segura la presencia de los procedimientos documentados sobre todas las tareas de rutina que se manejan dentro del área de TI, por lo cual, cuando un empleado de TI ingresa por primera vez, no tiene ese documento base, se le comenta que, de existir estos documentos, los tiempos en capacitación pueden reducirse de forma significativa y fue algo por lo cual se mostró bastante interesado.

Seguridad hospedada en la nube.

Cuando se le consultó al coordinador si conoce en su totalidad de todos los servicios que mantienen hospedados en la nube, indicó que no estaba seguro de conocer todos los productos existentes; en este caso, hizo mención de que se encuentra muy reciente en dicho puesto, por ello, de ahí se debe su desconocimiento. De igual forma, con este ejemplo queda demostrado la ayuda significativa que tendría si manejara la documentación adecuada para hacer la revisión de estos temas que son parte fundamental en el departamento tecnológico.

Revisión de las copias de seguridad de las bases de datos.

En cuanto a este tema, se consultó si se hace alguna revisión periódica donde se prueba que las copias de seguridad de las bases de datos, estén realmente íntegras y sean confiables e indicó que, en efecto, los respaldos se realizan de forma regular; inclusive, el sistema de Azure tiene configurado una automatización de respaldos; sin embargo, con estos, no se realiza ninguna prueba para comprobar que lo guardado sea realmente útil al momento de requerirse.

Políticas de restricciones para el uso de datos.

Se consultó si existen políticas de restricciones hacia el uso de los datos, por lo cual comentó que, en este caso, las restricciones las tiene configuradas cada perfil de puesto, pero que no se encuentra establecido como una política, sino como una tarea a realizar cada vez que se solicite.

Protección de sitios web.

Sobre la forma en que se encuentran protegidos los sitios web, el entrevistado explica que todos los sitios de la organización cuentan con su certificado de seguridad, representando accesos de confianza para los clientes.

Evaluación de equipos en amenaza.

Se preguntó al coordinador si tienen el control de los riesgos que pueden tener los equipos y si existe una forma de analizar cada equipo que se encuentra fuera de la organización por la forma virtualizada, en que se está trabajando. Comenta el entrevistado que existen dispositivos como el firewall y antivirus con los cuales se pretenden proteger los equipos de los riesgos a los cuales podrían estar expuestos, pero no existe ningún plan de evaluación de equipos, por tanto, se llegan a atacar los problemas en el momento en que ocurran, para evitarlo sí se realizarán planes de contingencia.

Gestión de riesgos por parte del proveedor.

Por parte del cliente, se consultó, y no se tiene el conocimiento apropiado sobre todas aquellas funciones que cumple el proveedor, con ello se demuestra que hay un compartimiento de funciones entre proveedor y cliente y, por ende, cabe la posibilidad

de que se dejen de hacer tareas de importancia, pensando en que cada una de las partes lo está gestionando.

Términos legales proveedor – clientes.

Se consulta acerca de si se firmaron acuerdos entre ambas partes, en caso de cesar el contrato, o bien, el conocimiento de los términos, en caso de ocurrir algún evento por parte del proveedor, que impida mantener los servicios en funcionamiento, a esto el coordinador indicó que desconocía los términos tanto sobre el proceder, en caso de querer terminar el contrato o bien, la forma en que se manejaría la confidencialidad de la información, en caso de ocurrir alguna eventualidad.

Reporte de Alertas en la plataforma de Azure.

Se hace la consulta sobre el tratamiento que se hace al sistema de alertas que la plataforma de Azure proporciona y el entrevistado hace constar que no hay ninguna persona encargada de ver ese tipo de eventos o alertas, dejando así, inconvenientes que probablemente puedan traer consecuencias graves de no tratarse con el tiempo debido.

Políticas para la eliminación de activos.

Según la respuesta por parte del encuestado sobre la existencia de políticas en cuanto a la eliminación de activos, y basándose en que él mismo desconoce del tema, se deduce que la organización no cuenta con ningún tipo de procedimiento a seguir en caso de desechar o bien eliminar algún activo presenten en la nube.

Gestión de perfiles y permisos de usuarios.

Se pregunta al coordinador sobre las normas a seguir para la creación de usuarios con sus respectivos permisos, a esto responde que los procedimientos se realizan con el cuidado debido, validando los permisos que deban darse según el perfil o grado de confianza del empleado; sin embargo, no existen ninguna documentación referencial para la gestión de perfiles y permisos de usuario.

Gestión de cambios.

Se interroga al encuestado sobre los procedimientos a seguir, en caso de que se deba dar algún cambio en cuanto a la configuración, cambios en permisos, gestión de contraseñas, etc., y su respuesta es que las tareas se realizan, una vez solicitado dicho

cambio, el correo electrónico es el medio que se utiliza para que los cambios estén totalmente respaldados por los encargados correspondientes, aunque no existe ningún control documental donde se demuestre por qué se realizó el cambio, cuáles fueron las partes interesadas y si afecta en cualquier proceso.

Revisión periódica de accesos.

Se hace la consulta de si para validar los accesos se cuenta con un cronograma, o bien, alguna estrategia de revisión sobre los derechos de acceso que tiene cada empleado; en este caso, el encuestado indica que dicha configuración se ejecuta y luego de ello no se da una revisión periódica para validar que aún se estén cumpliendo con los permisos establecidos o, por el contrario, verificar si era necesario agregar o quitar funciones o permisos.

Interpretación de los resultados de la observación

Con el método de observación, se realizó un análisis de la configuración de la plataforma de Microsoft Azure, dicho método se llevó a cabo durante 4 días y su fin fue comprender los parámetros que se encuentran configurados en los diversos recursos que la organización tiene contratados con su proveedor; además de revisar la existencia de amenazas que podrían generar algún riesgo significativo hacia la información que se controla desde la nube. A continuación, se expondrá detalladamente la información de lo observado durante los días indicados.

Figura 5. Puntuación de seguridad de la identidad

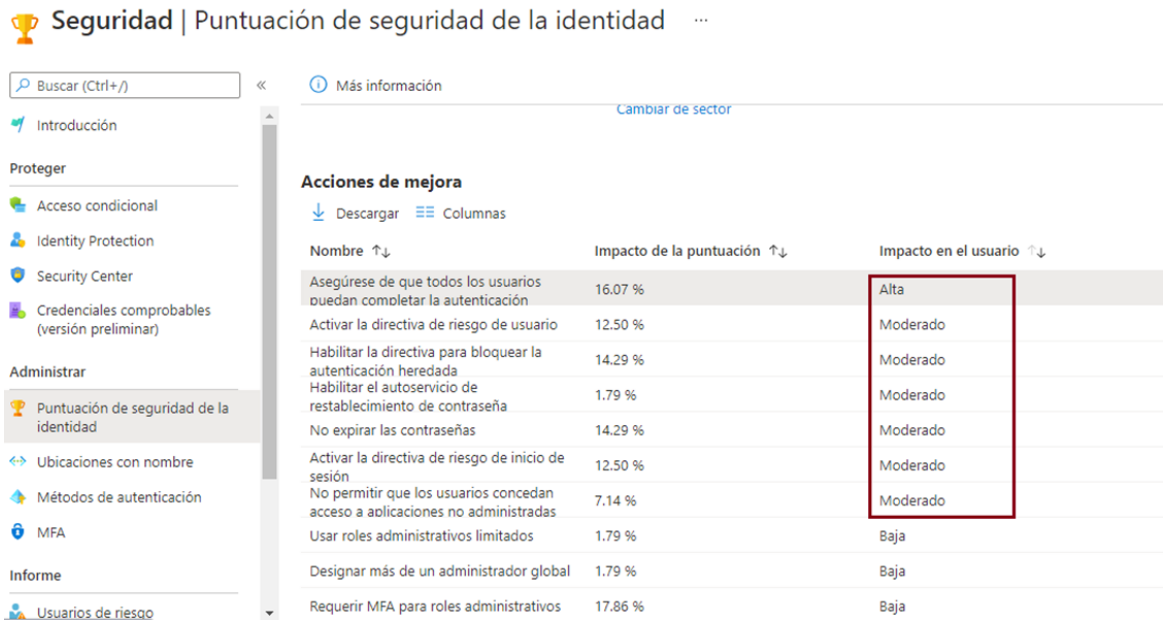

Figura 5. Usuarios de riesgo
Fuente: Nube de Azure PRICOSE

En términos generales, dentro de las primeras observaciones realizadas al centro de seguridad que tiene la configuración de Microsoft Azure, se descubrió la opción en donde Azure genera una puntuación con respecto a cómo se tiene configurada la identidad; esto representa la configuración de las credenciales de acceso, los riesgos de usuarios y todos aquellos temas referentes a la seguridad dentro de la organización. Sobre la puntuación que le brinda Azure a cada caso encontrado, le asigna un impacto clasificado en: alto, moderado y bajo. Para este apartado, se analizará cada observación según las tablas 1, 2, 3 y 4, en donde se referencia el número de observación por examinar.

Tabla 3. Bitácora de Observación – Día 1.

Bitácora de Observación				
Fecha de Observación: lunes 16 de agosto de 2021				
# Observación	**Herramienta observada**	**Detalle de observación**	**Resultado obtenido**	**Tiempo de ejecución**
1	Seguridad | Autenticación doble factor	Configuración adicional que se le solicita al usuario para iniciar la sesión segura. La puntuación máxima según Azure para este punto debe ser de un 9, la organización se encuentra en un 0,18.	La mayoría de los usuarios del AD no tienen el doble factor de autenticación, lo que incurre en mayores riesgos sobre la identidad.	15 minutos
2	Seguridad | Riesgo de Usuario	Control para el acceso de los usuarios. La puntuación máxima según Azure para este punto debe ser de un 7, la organización se encuentra en un 0.	Inexistencia de directivas de control de riesgos para impedir el acceso a los recursos en caso de una eventualidad.	10 minutos
3	Seguridad | Autoservicio de restablecimiento de contraseña	Herramienta que la plataforma provee para el envío de restablecimiento de contraseña a los usuarios. Azure clasifica este punto como moderado.	No existe la configuración para que el sistema envíe un correo de restablecimiento de contraseña en caso de ser necesario.	10 minutos

Tabla 3. Bitácora de Observación - Día 1.
Fuente: Elaboración propia.

Tabla 3. Bitácora de Observación – Día 1.

Bitácora de Observación				
Fecha de Observación: lunes 16 de agosto de 2021				
# Observación	**Herramienta observada**	**Detalle de observación**	**Resultado obtenido**	**Tiempo de ejecución**
4	Seguridad | Tiempo de expiración de contraseñas	Plazo de tiempo que se configura para que los usuarios cambien su contraseña.	La configuración de restablecimiento de contraseña se encuentra para que en un plazo de 6 meses la contraseña expire y el usuario deba cambiarla cuando la recomendación es que se maneje contraseña segura sin expirar.	5 minutos

Observación #1. Autenticación multi - factor.

Según Microsoft Docs (2021), la autenticación multi – factor es un medio sobre el cual se le pide al usuario alguna información adicional (código mediante un mensaje de texto al móvil, código a una cuenta de correo adicional, escaneo de la huella digital, entre otros), y de esta forma, lograr ingresar o iniciar sesión a las cuentas que se poseen.

Para este caso, y según se demuestra en la figura 5, el impacto que tiene la organización es alta, ello significa que la mayoría de los usuarios no cuentan con dichos factores múltiples para acceder a sus cuentas empresariales, a su almacenamiento empresarial y al chat mediante Microsoft *Teams*, lo que podría generar una amplia brecha de seguridad, dejando expuesta la información tenida en sus cuentas.

Observación #2. Directivas de riesgo de usuario.

Las directivas de riesgo en el usuario son las encargadas de automatizar las contestaciones a todo aquello que se detecta como riesgo, con dicha directiva se logra que los usuarios puedan corregir por sí mismos, los riesgos que el sistema detecte (Microsoft Docs, 2021).

Al revisar la configuración de las directivas de riesgo de usuario, dentro de la plataforma de Azure, se refleja que no se encuentra habilitada dicha directiva por lo que, la organización tiene con esta brecha, un impacto moderado que no está siendo mitigado y que el mismo Microsoft en la figura 5, lo está detectando como una acción de mejora.

Observación #3. Autoservicio de restablecimiento de contraseña.

Con el autoservicio de restablecimiento de contraseña, los usuarios consiguen cambiar sus contraseñas en el momento en que se necesite de una forma rápida y sin necesidad de que el administrador de la plataforma tenga que interponerse; por lo observado y según lo reflejado en la figura 5, la organización no cuenta con dicha configuración, esto significa que cuando los usuarios necesitan realizar sus cambios de contraseña, deben solicitarlo al departamento de TI para que se pueda realizar esta tarea; en este sentido, con solo el hecho de que sea el administrador que realice dicho cambio, la información de los usuarios puede ser interpretada por estar insegura. Adicional a ello, si los usuarios ante una emergencia requieren restablecer su contraseña y en ese momento la organización se encuentra en su día de descanso, estos deben esperar hasta que comience la jornada laboral para solicitarla, lo cual ocasionaría un entorpecimiento en un proceso.

Observación #4. Tiempo de expiración de contraseñas.

En la configuración de esta opción, se pudo observar que los usuarios cada seis meses deben estar cambiando sus contraseñas de las cuentas, esto provoca según la observación 3, que cada determinado tiempo todos deben estar llamando al departamento de TI para realizar dicho cambio y esto aparte de producir saturación en el soporte del departamento, Microsoft lo califica como innecesario y hasta de verse como una acción a mejorar con impacto moderado como lo muestra la figura 5.

Microsoft tiene predeterminada la forma para que las contraseñas no expiren, hacen mención de que estudios actuales indican que estos cambios en lugar de traer seguridad a las cuentas pueden causar más daño, pues induce a los usuarios a optar por contraseñas no tan seguras, inclusive a elegir la misma contraseña con un cambio insignificante, lo que puede ser fácil de predecir por parte de los ciberdelincuentes (Microsoft Docs, 2021).

Tabla 4. Bitácora de Observación – Día 2.

Bitácora de Observación				
Fecha de Observación: martes 17 de agosto de 2021				
# Observación	**Herramienta observada**	**Detalle de observación**	**Resultado obtenido**	**Tiempo de ejecución**
5	Seguridad | Directiva de riego de inicio de sesión	Directiva que se configura para evitar los inicios de sesión sospechosos.	Esta directiva se encuentra deshabilitada por lo que se está dejando una brecha para que personas externas puedan robar identidades y de esta forma iniciar la sesión.	5 minutos
6	Seguridad | Acceso aplicaciones integradas	Permitir a las diversas aplicaciones que tiene el usuario, acceder a la información en su nombre.	Se mantiene habilitada la opción de que las aplicaciones de terceros pueden hacer uso de los datos de la cuenta empresarial, ocasionando posibles riesgos de robo de información.	5 minutos
7	Seguridad | Roles de Administración limitados	Opción que permite tener distintos roles de administrador para que el acceso sea el realmente necesario.	No existe una configuración adecuada de los roles de los administradores.	15 minutos
8	Seguridad | Usuarios de riesgo	Listado que Microsoft Azure muestra para los usuarios que se encuentra con algún riesgo.	No se le da ningún tipo de continuidad ni procedimientos a seguir con el listado en riesgo.	10 minutos

Tabla 4. Bitácora de observación – Día 2.

Fuente: Elaboración propia.

Observación #5. Directiva de riesgo de inicio de sesión.

Al igual que en la observación 2 de la tabla 3, estas directivas pretenden automatizar a la mayor medida aquellas respuestas que se dan ante la presencia de riesgos de inicio de sesión. Para este apartado, la empresa no cuenta con una directiva para que, por medio de tareas automatizadas Azure, pueda detectar la autenticidad del usuario que está ingresando.

Observación #6. Acceso aplicaciones integradas.

Para Microsoft Docs (2021) las aplicaciones integradas: “pedirán a los usuarios permiso para acceder a los datos de la organización y los usuarios pueden elegir si se permiten” (párr. 2). En la configuración de Azure, esta opción se encuentra habilitada, sin embargo, no existen normas para manejarla de la forma recomendada por esta, lo que podría provocar el acceso a las aplicaciones por terceras personas, no autorizadas.

Observación #7. Roles de administración limitados.

Se observó referente a la tabla 5, que no existe una configuración y asignación de los roles de administración adecuados, se tiene un usuario administrador con acceso limitado a ciertas funcionalidades y no hay una clara percepción con el manejo de estos. Microsoft Azure, ofrece una lista amplia de roles para la administración del centro de operaciones de la plataforma, cada rol posee tareas en específico que pueden conceder acceso o bien denegarlo.

Observación #8. Usuarios de riesgo.

Cuando el servicio de Active Directory de Microsoft Azure identifica a un usuario en riesgo, es la alerta para el administrador de que esa cuenta puede estar con alguna afectación y significa algún tipo de riesgo para la organización. En cuanto a lo observado el martes, como se muestra en la tabla 2, desde la opción de “usuario en riesgo” y según la figura 6, se pudo detectar una lista significativa de usuarios que se encuentran en dicho estado. Más allá de que se encuentren en riesgo, la mayor preocupación es que no existe el personal para que vigile de una forma periódica, las diversas situaciones que están generándose.

Figura 6. Usuarios de riesgo

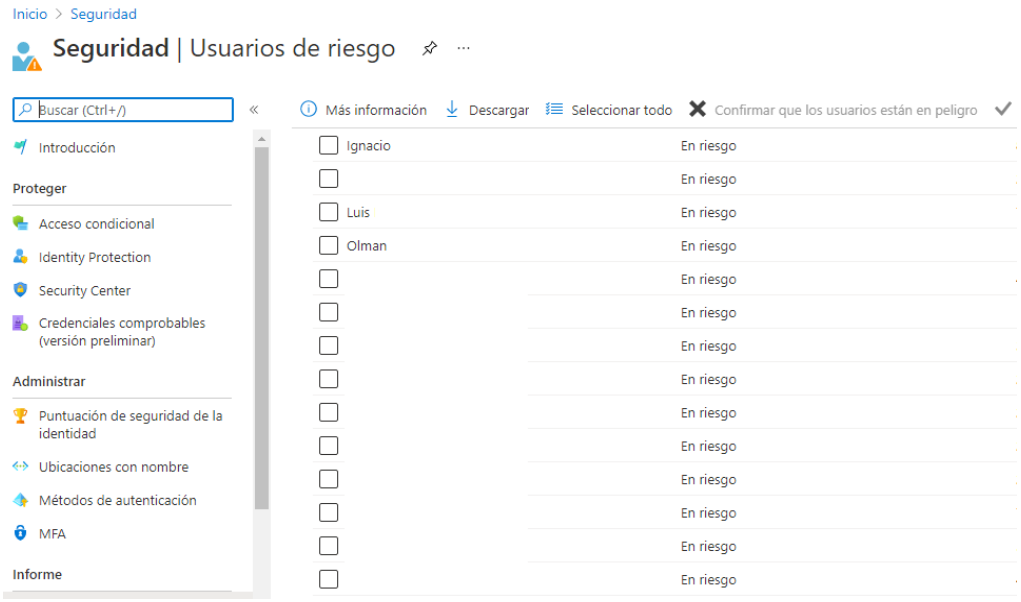

Figura 6. Usuarios de riesgo.
Fuente: Nube de Azure PRICOSE

Tabla 5. Bitácora de Observación – Día 3.

Bitácora de Observación				
Fecha de Observación: miércoles 18 de agosto de 2021				
# Observación	**Herramienta observada**	**Detalle de observación**	**Resultado obtenido**	**Tiempo de ejecución**
9	Autenticación | Protección con contraseña	Opción para la configuración de la protección que se le da a las contraseñas.	No existe una lista de contraseña prohibidas para que los usuarios no hagan uso de ellas al momento de hacer su cambio de contraseña.	10 minutos
10	Registro de aplicaciones	Aplicaciones de Azure con las que cuenta la organización.	Certificados de las aplicaciones se encuentran expirados y no hay una persona encargada de analizar el posible riesgo.	5 minutos
11	Análisis de cambios	Asistencia de Azure en donde detecta los cambios que sufre cada servicio.	No se tiene a ninguna persona responsable que pueda analizar cada cambio sufrido en la plataforma.	5 minutos

Tabla 5. Bitácora de observación - Día 3.

Fuente: Elaboración propia

Tabla 5. Bitácora de Observación – Día 3.

Bitácora de Observación				
Fecha de Observación: miércoles 18 de agosto de 2021				
# Observación	**Herramienta observada**	**Detalle de observación**	**Resultado obtenido**	**Tiempo de ejecución**
12	Máquina Virtual | Seguridad	Supervisión de la configuración de las máquinas virtuales para la identificación de vulnerabilidades.	Disco duro sin cifrar Agentes sin instalar Protección de conexión Puertos de red sin restringir Evaluación de vulnerabilidades deshabilitada Puertos de administración abiertos	15 minutos

Observación #9. Protección con contraseña.

Figura 7. Protección con contraseña.

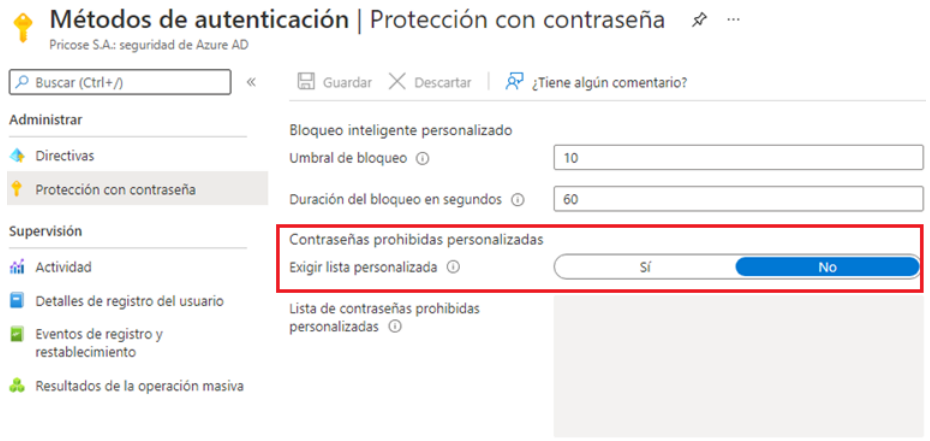

Figura 7. Protección con contraseña.
Fuente: Nube de Azure PRICOSE

Según la observación que se realizó el miércoles referente a la tabla 6, se pudo detectar que el sistema en la opción de la protección con contraseña, indicada según la figura 7, no tiene habilitado el listado de las contraseñas restringidas (contraseñas que el administrador ingresa para que ningún usuario pueda utilizarlas), lo que tiende a producir, es que los usuarios puedan generar contraseñas de muy baja complejidad lo cual implica riesgos para aquellos datos que se encuentran alojados en la nube.

Observación #10. Registro de aplicaciones.

En la opción del registro de las aplicaciones que tiene Microsoft Azure en la compañía, en la tabla 6, se detectó que algunas de ellas no cuentan con un certificado de seguridad actualizado, el sistema las muestra como expirado, tal como se refleja en la figura 8, lo que pudiese generar desconfianza en los clientes, al tratar de acceder al sitio.

Figura 8. Registro de aplicaciones (certificados).

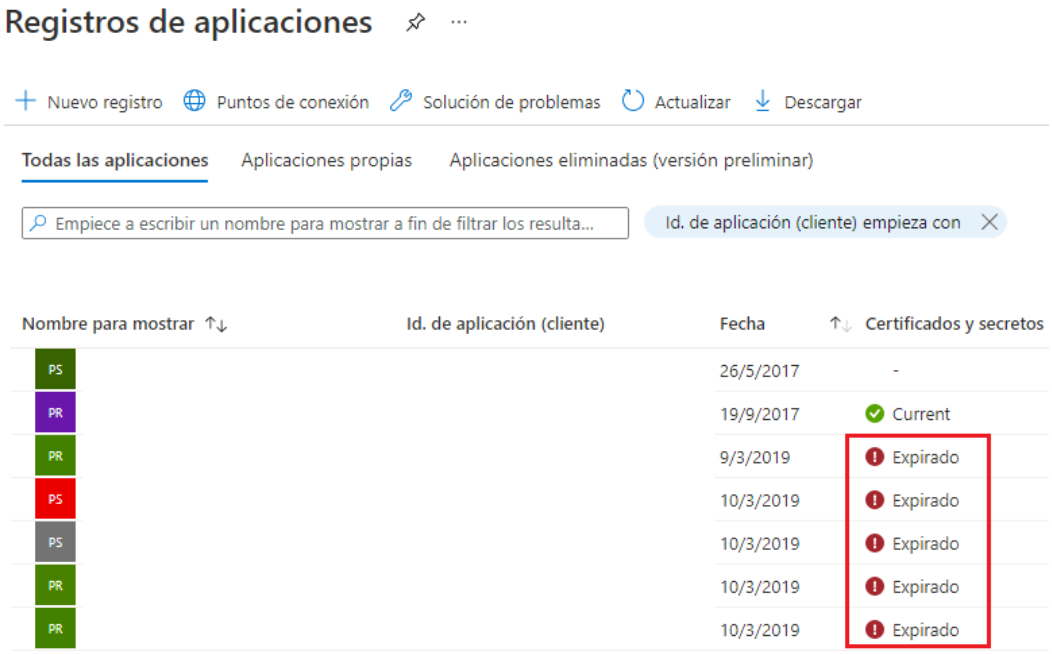

Figura 8. Registro de aplicaciones.
Fuente: Nube de Azure PRICOSE

Observación #11. Análisis de cambio dentro de la plataforma Azure.

Microsoft Azure cuenta con una cantidad de opciones para realizar análisis de cambios que han sufrido las aplicaciones, sin embargo, PRICOSE no posee una persona encargada a nivel interno para ver estos procesos y validar que los cambios sean los correctos y que los haya hecho el usuario correspondiente y en el momento adecuado.

Observación #12. Seguridad en máquinas virtuales.

Al momento de revisar la configuración de las máquinas virtuales, según la tabla 12, se notó una serie de acciones por mejorar según las recomendaciones que indica Azure. Estas acciones se encuentran en orden de prioridad, y se observa en la figura 9 que existen acciones para mitigar el alto y medio riesgo. Al igual que en observaciones anteriores, este tipo de análisis no está siendo examinado por ninguna persona del área de TI.

Figura 9. Seguridad en máquinas virtuales

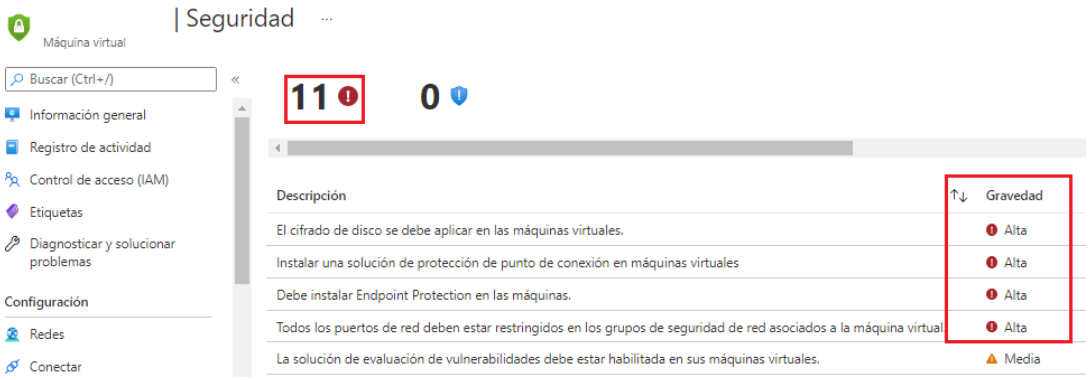

Figura 9 Seguridad en máquinas virtuales.
Fuente: Nube de Azure PRICOSE

Tabla 6. Bitácora de Observación – Día 4.

Bitácora de Observación				
Fecha de Observación: jueves 19 de agosto de 2021				
# Observación	**Herramienta observada**	**Detalle de observación**	**Resultado obtenido**	**Tiempo de ejecución**
13	Roles | Control de acceso	Administración de control de acceso que se le otorga a los usuarios sobre los servicios de Azure	La configuración de asignación de roles para el control de acceso solo esta para el usuario administrador y para las aplicaciones, no se refleja para los demás usuarios; esto a pesar de que Azure maneja un listado de roles específicos.	10 minutos
14	Seguridad | App *Service*	Aplicaciones de Azure con las que cuenta la organización	Solicitud de certificado No este habilitado el cumplimiento FTPS Acceso sin https Registros de diagnóstico deshabilitados	15 minutos
15	Seguridad | Cuenta de almacenamiento	Archivo Digital de la organización	No existe una conexión de vinculo privado No hay restricciones de acceso Acceso público	10 minutos

Tabla 6. Bitácora de observación - Día 4.

Fuente: Elaboración propia.

Observación #13. Roles – Control de acceso.

Como se puede observar en la figura 10, en la nube de Azure las organizaciones disponen de una lista amplia de roles, para que de esta forma se asignen los permisos a los usuarios según sus funciones. Cuando se revisa el control de acceso según la cantidad de roles que hay (correspondiente a la figura 11), se refleja que las directivas solamente se han creado para las aplicaciones y para el usuario administrador, por lo cual, según demostración en la observación 13 de la tabla 8, no existen directivas de acceso para los demás usuarios, incluyendo al departamento de TI.

Figura 10. Roles de control de acceso

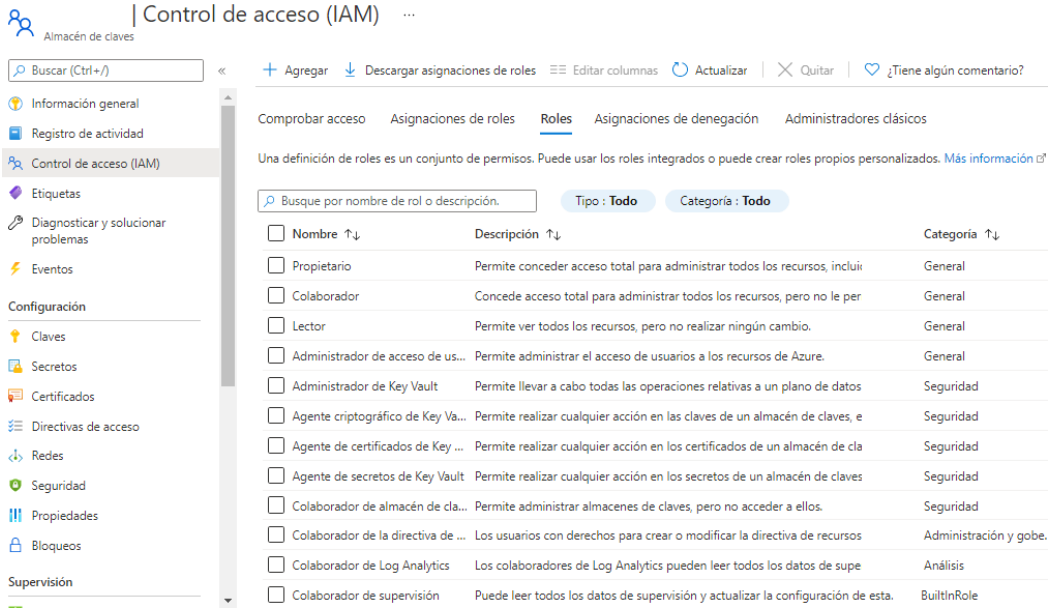

Figura 10. Roles de control de acceso.

Fuente: Nube de Azure PRICOSE

Figura 11. Asignaciones de roles

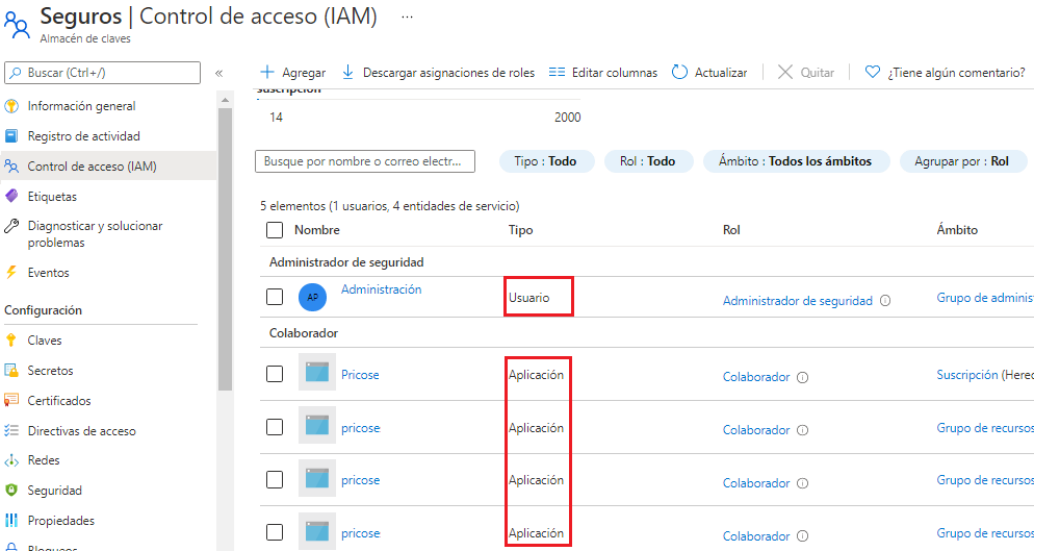

Figura 11. Asignación de roles.

Fuente: Nube de Azure PRICOSE

Observación #14. Seguridad – App *Service*.

Dentro de los servicios que la organización posee en la nube, se encuentran los App *Service* y Azure (2021) los define como: "un servicio de hospedaje web totalmente administrado que permite crear aplicaciones web, servicios y API *RESTful*. El servicio ofrece un amplio abanico de planes para satisfacer las necesidades de cualquier aplicación, desde sitios web pequeños hasta aplicaciones web a escala mundial" (párr. 20).

En ese caso, similar a las observaciones anteriores, se refleja una serie de mejoras en cuanto a la configuración, acciones que hay que darle un alta, medio o leve importancia según lo demuestra la figura 12.

Figura 12. Seguridad – App *Service*

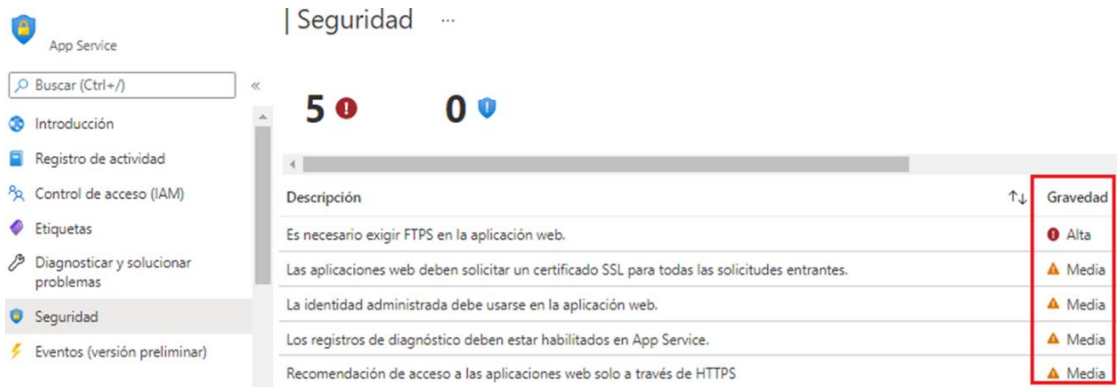

Figura 12. App Service.

Fuente: Nube de Azure PRICOSE

Observación #15. Seguridad – Cuenta de almacenamiento.

El almacenamiento de los datos en PRICOSE, se manejan mediante un File Server (servidor de archivos locales) y por medio de cuentas de almacenamiento en la nube de Azure. En la imagen 13 se observa la configuración de una de las cuentas de almacenamiento que la organización posee, pero al igual que en las demás observaciones, nadie se encuentra a cargo de atender las advertencias que se presentan al mantener estos servicios. Se logra ver que hay medidas correctivas que son de prioridad atender como lo es un permiso de acceso público que se mantenga habilitado sin tener ninguna restricción para su acceso.

Figura 13. Cuenta de almacenamiento

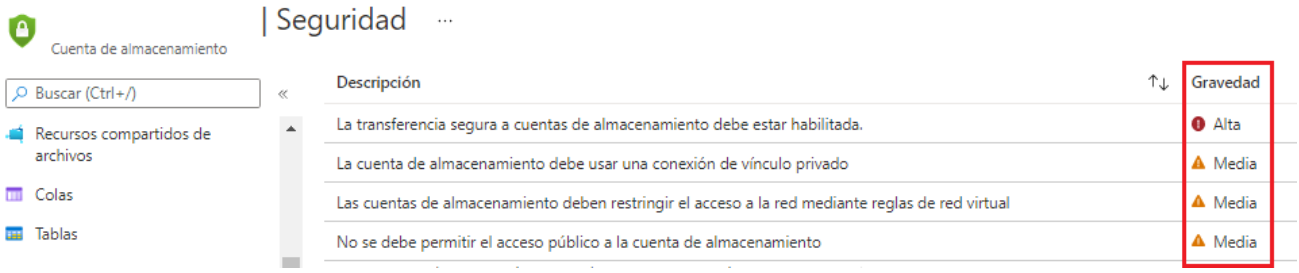

Figura 13. Cuenta de almacenamiento

Fuente: Nube de Azure PRICOSE

Con respecto a los resultados en los tres instrumentos aplicados, se puede deducir que la empresa PRICOSE, carece de controles para identificar cuáles son las responsabilidades específicas de cada puesto, en especial del área de tecnología y es necesario realizar una separación de funcione; asimismo, se puede mejorar la forma en que se realizan los procesos, pues se demostró que sus actividades la realizan por defecto; sin embargo, no existe ningún tipo de documentación para respaldar lo realizado. Es necesario tratar la seguridad de la información con respecto a los respaldos que se realizan; además, es importante atender la lista de observaciones que la plataforma de Azure les está alertando. Asimismo, se debe generar conciencia de que la responsabilidad de su seguridad no solo depende del proveedor, por el contrario, es necesario atender la administración de dicha plataforma y asignar a personas responsables de estas gestiones. Por lo tanto, el proponer una implementación de normas de seguridad, se llegan a cerrar muchas de las brechas presentes para la organización y que hoy en día, no se están atendiendo con la eficacia y eficiencia necesarias.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

En el presente apartado, se expondrán las conclusiones que se dieron luego de realizar el estudio de análisis de los resultados, sobre los instrumentos aplicados y según la propuesta elaborada; adicionalmente y conforme a lo observado y estudiado en los resultados y sobre el conocimiento adquirido, se desarrollará una lista de recomendaciones por tomar en cuenta para que la organización, pueda tener una referencia de los procedimientos a seguir y de esta forma, mitigar aquellos casos necesarios para lograr una mejor seguridad con respecto a la información alojada en la nube.

Conclusiones.

A la vista del trabajo ostentado, a continuación, se detallan las principales conclusiones de la propuesta; se hace referencia a la información encontrada, luego del análisis de los resultados y de los logros alcanzados sobre las políticas de seguridad de la información:

1. Se logró diseñar una propuesta para PRICOSE con el fin de implementar la seguridad de la información de los servicios en la nube, mediante una serie de normas establecidas por la ISO 27017 y de la mano con las normas ISO 27002.
2. Con la ejecución de las variables indicadas en la propuesta, se logró la recolección de información valiosa, brindada por los empleados de la organización; se genera así un panorama más amplio sobre la problemática existente y se da fe a lo descrito en el planteamiento del problema.
3. Por medio de la interpretación de resultados de la observación, fue posible comprender el entorno de trabajo que la organización mantiene en su administración de nube, se identifica de esta forma, una cantidad importante de riesgos que pueden afectar la seguridad de los procesos y datos operados en esta.
4. Con la elaboración del instrumento de la entrevista, se estableció una conversación directa con el encargado de TI en donde, mediante la realización de preguntas sobre la operativa del departamento, se descubrió que no hay una clara percepción sobre las directrices que se deben manejar para un uso óptimo de los datos y de los activos de la organización, con lo cual se ayuda a tener una mejor conciencia sobre cómo debía ir desarrollándose la propuesta.

5. Se realizó un análisis de los tipos de información que la organización maneja en la nube; luego de ello, se procedió a clasificarlos según su confidencialidad, disponibilidad e integridad; se logró de esta forma, minimizar el riesgo de fuga de datos para brindar la protección oportuna, según el tipo de sensibilidad que esta maneje.
6. Mediante el análisis de los resultados, se reflejó una necesidad de formación para el departamento de TI sobre el manejo de los servicios adquiridos en la nube y la aclaración sobre las responsabilidades que le competen a estos como organización y al proveedor de dicho servicio; de esta forma, se obtendrá una percepción más clara sobre los recursos que existen para que puedan ser aprovechados, ya que la organización está pagando por recursos que no son usados o consumidos en su totalidad.
7. Se formaron los roles y con ello, la definición de sus responsabilidades, referentes al control de la seguridad de los datos que deben ser gestionados y resguardados en la nube; se deja entre los roles más destacados, una comisión que vele por todo lo pertinente con la seguridad de la información y un gestor de seguridad como el principal responsable para que lo indicado en la propuesta, se lleve a cabo.
8. Teniendo de manera organizada el análisis de resultados y con la guía de las normas ISO 27017 Y 27002, se elaboraron las políticas que más se adecuaban a la organización y a su forma de trabajo en la administración de la nube, con lo cual se obtuvieron pautas claras para la administración de los recursos y de los datos, así como la asignación de los responsables, los compromisos que se deben cumplir para una gestión y clasificación de activos, la creación de controles de acceso, la definición de las pautas a seguir para trabajar con los proveedores, entre otras políticas; con ello se cumplió con el objetivo general y los objetivos específicos propuestos en este proyecto.

Recomendaciones.

Según la experiencia sobre lo desarrollado en este trabajo y con base en los hallazgos descritos, se sugieren las siguientes recomendaciones para tomar en cuenta en la organización:

1. La principal recomendación es la de aplicar las normas de seguridad propuestas, para avalar la integridad, confidencialidad y disponibilidad de los datos, tomando en razón que cualquier sistema o recursos de TI que no cuenta con medidas de protección, pueden ser vulnerados en cualquier momento; lo anterior se analizará en enero del año 2022. Dicho análisis será responsabilidad del sustentante de este proyecto, en compañía del departamento de TI y el Gerente General, para llevar la propuesta a la Junta Directiva de PRICOSE.
2. Cualquier empleado, indiferentemente del área, debe tener clara la importancia de resguardar y gestionar los datos y activos de la organización, por lo que se recomienda aprovechar el taller de concienciación que se logró negociar con uno de los proveedores; dicho taller totalmente gratuito y para todo el personal de la empresa, será impartido por el proveedor, siendo responsable de la coordinación el encargado de TI. El taller se debe coordinar con un mes de anticipación, por lo cual se recomienda ejecutar entre los meses de febrero o marzo del año 2022.
3. Dentro del departamento de TI, se tienen que definir claramente las funciones que ejecuta cada empleado, con el fin de que el compromiso sobre la seguridad de la información sea compartido por todos los miembros, pero con tareas específicas asignadas a cada uno, tomando en cuenta, que dicho departamento se compone de una cantidad limitada de trabajadores. El cumplimiento de estas funciones estará bajo la responsabilidad del encargado de TI, en compañía del gestor de seguridad de la información, con una duración de 3 semanas; luego de los cambios acordados, se deberán divulgar las decisiones a los interesados.
4. El encargado de TI debe asegurarse de que las normas aquí establecidas estén a disposición de todos los empleados, y/o terceras personas (de ser necesario); este proceso se realizará una vez efectuada dicha etapa, con duración de una semana; adicionalmente, deberá dar el seguimiento ante las dudas y consultas que puedan presentarse por parte de los interesados.
5. Desarrollar un plan de trabajo para la implementación de las políticas de seguridad, este plan será asumido por el sustentante de este proyecto con el

apoyo del departamento de TI, dicho plan debe ser realizado durante el primer trimestre del año 2022.

6. Se recomienda realizar un análisis exhaustivo de los demás riesgos presentes en la plataforma de Azure y no documentados en esta propuesta, esto sobre los activos que se encuentran en la nube, con el fin de atender estos riesgos oportunamente y tratar de minimizar su impacto dentro de la organización; así como ejecutar el plan de acción por seguir, según el grado de importancia que los resultados muestren; dicho análisis estará a cargo del encargado de TI y se deberá efectuar durante el mes de enero del año 2022.
7. Debido al alcance del proyecto y la magnitud que es implementar la gestión de recursos humanos, se recomienda que para una segunda etapa dicho tema se integre dentro de las políticas propuestas; lo anterior estará bajo la responsabilidad de la comisión de seguridad de la información, con el apoyo del encargado de recursos humanos de la empresa con un tiempo aproximado de 6 meses.
8. Se recomienda segregar los roles de TI, específicamente, para que haya una persona responsable de atender los ambientes de producción y otra atienda los de pruebas, con el objetivo de mejorar el nivel de seguridad de la información. Esta responsabilidad debe asumirla el encargado de TI con el apoyo de gestor de seguridad de la información a un plazo no mayor a una semana, luego de entregada esta primera etapa.
9. Se sugiere al encargado de TI, examinar las alertas encontradas y recomendaciones dadas por el mismo servicio de la nube, para tomar las acciones adecuadas que minimicen las posibles amenazas existentes, lo anterior a un plazo no mayor a 3 semanas del mes febrero 2022; luego de ello, seguir las recomendaciones de tiempos establecidos en esta propuesta.

CAPÍTULO VI: PROPUESTA

En el presente capítulo, luego de analizadas las oportunidades de mejora de las cuales se puede beneficiar la organización para asegurar sus datos que se encuentran hospedados en la nube; se ejecutará la propuesta en donde se pretende proponer la implementación de la seguridad de la información por medio de un catálogo de medidas y controles referenciados por la norma ISO 27017. Esta norma está constituida en un formato similar a la norma ISO 27002, incluyendo las cláusulas del 5 al 18 y adicional a estas, se agregan 7 controles más. A continuación, se presentan las cláusulas que se tomarán en cuenta, para el desarrollo de esta propuesta:

1. Políticas de seguridad de la información
2. Organización de la seguridad de la información
3. Gestión de activos
4. Control de acceso
5. Seguridad de las operaciones
6. Seguridad de las comunicaciones
7. Adquisición, desarrollo y mantenimiento de sistemas de información
8. Política de seguridad de la información relacionada con el proveedor
9. Gestión de continuidad del negocio
10. Cumplimiento
11. Conjunto del control extendido del servicio en la nube

Pricose Primera Sociedad Agencia de Seguros S.A.

Control de versión en las Políticas de la Seguridad de la Información en la nube

Versión	Fecha	Realizado por	Detalle	Firma
V-1.0				

Objetivo.

Establecer políticas sobre el uso que se le da a la información y la forma en que será compartida, basado en la norma ISO 27017.

Política de Seguridad de la información.

Generalidades de las políticas.

Las políticas de seguridad de la información son las creaciones de un conjunto de normas o reglas que deben ser respetadas por el personal de la organización para lograr acceder a la información y a los recursos de la empresa. Dichos documentos deben ajustarse a las necesidades de cada organización, y su revisión debe ser de forma continua (Scielo, 2008).

Documento de la política de seguridad de la información.

Las políticas, una vez establecidas, deben aprobarse por las altas direcciones para mostrar el compromiso que se tienen por estas y luego, se deben comunicar y publicar a todos los empleados de la organización, así como a las personas externas.

Objetivos de control.

Resguardar de una forma íntegra, confiable y confidencial la información y los recursos que se manejan en la empresa PRICOSE, Primera Sociedad Agencia de Seguros, S.A, mediante el uso de políticas establecidas para todo el personal

Alcance

Dichas políticas son adaptables a todos los funcionarios de PRICOSE, contratistas y personas externas que llegan a utilizar la información, tecnologías y recursos de la empresa, estas deberán ser de cumplimiento obligatorio y de comprensión para el lector.

Declaración de la política general de seguridad de la información.

Pricose, Primera Sociedad Agencia de Seguros, S.A, reconoce la importancia que tiene la seguridad de la información que poseen en la nube y el manejo de los procesos de la organización. Para amparar la seguridad de la información, la empresa se deberá comprometer a:

- Suministrar los recursos precisos para la implementación de la política indicada.
- Divulgar la política de seguridad de la información a las partes interesadas.
- Promover de manera activa los objetivos de la política.

- Desenvolver y ejecutar un plan de mejora continua con el propósito de generar una adecuada gestión sobre la política.

Información adicional.

En caso de que la política de la seguridad de la información tenga que ser divulgada hacia personas o entidades fuera de PRICOSE, es requerido manejar con el cuidado debido la confidencialidad de la información, lo anterior para que no se expongan datos que puedan poner en algún riesgo a la organización.

Revisión de las políticas.

El proceso de revisión de las políticas que se establezca se deberá someter a una revisión de al menos una vez por año y se actualizarán cada vez que exista un cambio relevante para la organización en donde se pueda ver en riesgo la seguridad de la información.

Objetivos de control.

Estos cambios, primeramente, tendrán que ser revisados por el Departamento de Tecnología de PRICOSE, para que consecutivamente se aprueban por la Gerencia y Junta Directiva según el cuadro de revisión de aprobación de las políticas de seguridad de la información, referenciado mediante el apéndice 5, en donde, para la columna de rol se despliega una lista seleccionable según el proceso realizado:

- Creación. Persona quien creó la política.
- Revisión. Persona que revisó la política luego de creada.
- Aprobación. Gerente, quien aprueba lo indicado en la política
- Autorización. Miembro de la Junta Directiva, autorizando para su divulgación, ejemplificado en la imagen 14.

Figura 14. Roles de la aprobación de las políticas de la seguridad de la información.

Figura 14. Roles de aprobación de políticas.

Fuente: Elaboración propia.

Conformación de la comisión de seguridad de la información.

Se deberá conformar una comisión de seguridad de la información, con el objetivo de velar por que las funciones establecidas en la política se lleven de una forma transparente; con respecto a dicha creación, se establece el formato con la información necesaria mediante el apéndice 6 y es el encargado del área de TI quien convocará a las sesiones de trabajo en dicho comité. Entre las principales funciones de la comisión serán:

- Revisión de los cambios más relevantes que se presenten en donde se ponga en riesgo la seguridad de la información.
- Aprobar las solicitudes indicadas por el Departamento de Tecnologías de la Información en donde demuestren que su fin es dar seguridad a la información.
- Establecer procedimientos específicos en beneficio a la seguridad de la información.
- Velar por el buen funcionamiento de las políticas creadas.
- Revisar al menos una vez al año las políticas establecidas.
- Revisar y aprobar las políticas de seguridad de la información.
- Apoyar con la divulgación de las políticas hacia toda la organización.

- Efectuar revisiones sin un previo aviso y de forma aleatoria a los departamentos de la organización, con el fin de evaluar si están cumpliendo con lo indicado en las políticas.
- Denunciar cualquier incumplimiento que pueda darse sobre la política general y las políticas específicas, agrupadas a esta.
- Plantear mejoras a las políticas según el conocimiento y la necesidad de la organización.

Cuando se efectúe una revisión de las políticas, es favorable que se tomen en cuenta los resultados de la revisión obtenida por parte de la comisión de seguridad de la información, así como las oportunidades que se presenten para mejorar las políticas de seguridad, por lo tanto, será obligación de la comisión generar mejoras:

En los objetivos de control y de los controles en sí.

En la asignación de los recursos y en las responsabilidades asignadas.

En la dirección de la organización con respecto a la seguridad de la información, alineados a los objetivos y metas de PRICOSE.

Marco de referencia.

Para el desarrollo de las políticas de seguridad de la información alojada en la nube, se toma como referencia el marco de las Normas ISO, en específico para el caso de la computación en la nube, la ISO 27017 en conjunto con las normas establecidas en la norma ISO 27002.

Aspectos generales.

Esta norma se compone por una lista de modelos sobre los aspectos específicos de la seguridad de la información, incluyendo los siguientes apartados:

Organización de la seguridad.

Gestión de activos.

Control de acceso.

Seguridad de las operaciones

Seguridad de las comunicaciones

Adquisición, desarrollo y mantenimiento de los sistemas de información.

Políticas de seguridad de la información en relación con proveedores.

Aspectos de la seguridad de la información en la continuidad del negocio.

- Cumplimiento con los requisitos legales.
- Funciones y responsabilidades compartidas dentro de un entorno de computación en la nube.
- Eliminación de activos del cliente del servicio en la nube.
- Monitoreo de servicios en la nube.
- Alineación de la gestión de la seguridad para redes virtuales y físicas.

Sanciones por incumplimiento.

Ante el incumplimiento de las políticas de seguridad de PRICOSE, se aplicarán las sanciones que se encuentran establecidas en la política interna de trabajo, página 46, título XIV "Sanciones Disciplinarias" que comprende del artículo 85 al 90.

Control de cambios.

Al momento de requerirse algún cambio significativo en las políticas, estas aparte de su aprobación, deberán de monitorearse mediante el documento de control de cambios en la organización, en el apéndice 7 se establecerá el formato para dicha gestión.

Políticas específicas por desarrollar en la seguridad de la información.

Una vez establecido los procesos a seguir para la creación de las políticas, se desarrollarán las políticas generales, necesarias para el resguardo de la información alojada en la nube. El listado de las políticas, a continuación:

- Políticas de contraseñas.
- Políticas de uso de la información y de los recursos informáticos.
- Políticas del uso de Internet y correo electrónico.
- Políticas de uso de la Intranet y Sitio Web de PRICOSE.
- Políticas para Desarrolladores de Software.
- Políticas para Administradores de Sistemas.
- Políticas con el proveedor de servicio en la nube.

Políticas de contraseñas.

El uso de las contraseñas representa un método básico que el Departamento de Tecnologías de la Información debe brindar a cada usuario de PRICOSE, para que

utilice de una forma correcta, la autenticación a las plataformas ofrecidas por la compañía.

Objetivos de control.

- Cuando se realice un cambio de contraseña, esta no debe ser igual a sus últimas 8 contraseñas.
- La longitud de las contraseñas debe ser de al menos 12 dígitos, alfanuméricos en donde se deba utilizar como mínimo una letra en mayúscula, una letra en minúscula, numeraciones (0 – 9) y caracteres especiales (-, *, /, entre otros).
- No se permiten contraseñas que hagan referencia a su nombre, apellido, usuario de cuenta de correo, ni palabras alusivas al negocio como: seguros, pricose, oficina, entre otras.
- Es responsabilidad del usuario mantener las contraseñas en un lugar seguro y sin acceso hacia los demás.
- El cambio de contraseñas debe ser únicamente al usuario que le corresponde.
- Los usuarios no deberán emplear una misma contraseña para las distintas aplicaciones que le brinda la organización.

Políticas de uso de la información y de los recursos informáticos.

Las políticas del uso de la información y de los recursos deben someterse a todas las instrucciones que imparta la comisión de seguridad de la información.

Objetivos de control

- El uso de la información de la compañía debe ser única y exclusivamente con propósitos del cumplimiento de las labores asignadas y para negociaciones anteriormente autorizadas.
- No es permitido compartir ningún tipo de contraseña, acceso, pantalla o acceso remoto a personas externas de la empresa.
- La información con la que se trabaja debe ser de uso confidencial y, por lo tanto, ninguna divulgación de esta es permitida, a menos que sean para fines de negociación entre la compañía, INS – PRICOSE, proveedores – PRICOSE, lo anterior con la debida autorización que el puesto posea.

- Cuando necesite distanciarse de su lugar de trabajo sea dentro como fuera de la institución, es requerido que aplique la opción de bloqueo de pantalla a su computador.
- Es prohibido el retiro, la divulgación, el cambio y el compartimiento de la información que es almacenada en medios removibles como lo son los USB, discos, entre otros.
- Es prohibido el uso del software que le brinda la compañía, para fines personales, a menos que exista una autorización por parte de alguna jefatura autorizada.
- Es prohibido la instalación y uso de software adicional al que la organización le brinda, de ser necesario alguna instalación, debe ser gestionado por el Departamento de Tecnologías de la Información.
- Es prohibido capturar contraseñas o la utilización de cualquier componente de control de acceso que le permita tener privilegios de entradas no autorizadas.
- No debe conservar ningún tipo de copia de información con la que usted trabaja, si no es por medio de los accesos compartidos que la misma compañía le brinda, y en ninguna circunstancia, esta información debe estar copiada en su computador o medios removibles personales.
- Es responsabilidad del personal mantener en buen estado los recursos que se le han asignado para la ejecución de sus labores.
- Es responsabilidad del personal informar al Departamento de Tecnologías de la Información ante cualquier tipo de inconveniente con la información y los recursos con los que trabaja.
- Cuando un colaborador cese su relación con la compañía, es responsabilidad del encargado de T.I. revisar la documentación, cuenta de correo, accesos y otros medios, para establecer la persona que se encargara del manejo de estos, o bien para su destrucción en caso de ser necesario.

Políticas del uso de internet y del correo electrónico.

El correo electrónico e internet son medios valiosos utilizados como una herramienta de marketing en las organizaciones y es por esto, que el cuidado y uso que se le dé a dichas herramientas son de los temas fundamentales que el área de TI debe proteger.

Objetivos de control

- El uso de internet y del correo electrónico debe ser exclusivamente con fines laborales y se deben tomar las medidas necesarias de protección para resguardar la información que se maneje de la organización.
- Cualquier uso de internet fuera de lo laboral, deber estar admitido y fundamentado por el encargado inmediato del usuario y a su vez, debe ser controlado por el Departamento de TI.
- Es permitido el intercambio de información, datos o archivos por medio de internet, siempre y cuando sean con propósitos laborales y con la seguridad que el Departamento de TI le haya indicado.
- Es responsabilidad del empleado el manejo que se le dé al uso del correo electrónico se da por entendido que, por ser un medio de comunicación de la organización, debe trabajarse con la formalidad que este merezca.
- La cuenta de correo asignada es de uso individual por lo que ningún otro empleado o persona debe tener acceso a este.
- Es responsabilidad del empleado informar al Departamento de TI sobre el espacio disponible en el buzón, información que el mismo correo le indica cuando ya se encuentra en su límite de espacio.
- Es responsabilidad del empleado revisar diariamente y de forma concurrente su bandeja de entrada, para el trato oportuno de los correos recibidos.
- No es permitido utilizar la cuenta de correo electrónico para el envío o recibido de correos con mensajes políticos, religiosos, humorísticos, sexuales, o bien, con algún fin personal.
- Es responsabilidad del empleado dar aviso de forma inmediata al Departamento de TI sobre correos que sean sospechosos, así como el acatamiento de las recomendaciones que el área crea pertinente.

Políticas del uso de la intranet y del sitio web de PRICOSE.

La organización maneja su intranet por medio de los servicios en la nube para la propagación de documentos que son utilizados entre esta y el colaborador, por lo que es responsabilidad del empleado, ingresar a la intranet para el uso de la información requerida.

Objetivos de control.

- La divulgación de las marcas, logos y cuanta información sea referente a la organización, solo se podrá utilizar en los sitios y sistemas web que la representada maneja; en caso contrario, se debe solicitar el visto bueno de las altas gerencias para su uso.
- El manejo de enlaces y conexiones de los sitios de la organización no son para uso particular del personal a excepción que se cuente con una autorización por parte de la gerencia.

Políticas para los desarrolladores de software.

El impulso de los sistemas informáticos es de gran apoyo para las actividades en que la empresa desenvuelve y es por eso, que se requiere de una norma para regular la forma de actuar entre proveedor del desarrollo y cliente.

Objetivos de control

- Los sistemas informativos en la organización deben contar con 3 ambientes del sistema, el de desarrollo, el de producción y el de pruebas, cualquier cambio que se deba realizar o probar primeramente debe estar en la BD de pruebas, en ninguna circunstancia este tipo de pruebas se debe realizarse bajo el ambiente de producción.
- Es responsabilidad del encargado de proyectos mantener la documentación renovada sobre los cambios o actualizaciones que el ambiente de producción sufra, así como de las pruebas que se realizan sobre el ambiente de pruebas.
- Es responsabilidad del encargado de proyectos velar porque se hagan las pruebas respectivas de la BD antes que sean puestas en producción.
- Se debe comprobar la seguridad de los datos y de conexiones que tendrá el ambiente de producción antes de entrar en operación.
- No se debe guardar ningún tipo de contraseña en el código del software, esto para que sea el mismo usuario quien la gestione.
- El encargado de proyectos debe velar porque el acceso que tenga cada usuario es el que le corresponda, según sus privilegios de uso; por ningún motivo los usuarios deben tener opciones que no correspondan en los sistemas.

- Cualquier adicional, modificación o eliminación de información sensible en los sistemas de la organización, debe estar registrada y documentada.
- El sistema deberá ser capaz de registrar los eventos de seguridad que esta sufra, y el encargado asignado, debe velar por la actuación oportuna ante dichos eventos.
- Los intentos de ataques ante la eliminación, creación o modificación de eventos deben estar controlados y con la seguridad que este amerite.
- Los registros que arroje el sistema deben estar únicamente disponibles para el personal que maneje la auditoría de los sistemas informáticos de la organización.
- Las modificaciones de la información que maneje el sistema deben ser exclusivamente para los usuarios con dichos privilegios, para evitar que cualquier tipo de usuario pueda modificar información sensible.
- Es responsabilidad del desarrollador validar las entradas que tenga el código con el propósito de evitar la exposición ante riesgos que pueda tener la seguridad.

Políticas para administradores de sistemas.

La administración de los sistemas debe ejercerse bajo un responsable liderazgo, siempre de acuerdo con la estrategia del negocio y de la mano con los reglamentos que la compañía crea pertinentes.

Objetivos de control

- El administrador, al momento de otorgar contraseñas a los usuarios, deberá ser exclusivamente en el primer ingreso; luego de ello, el sistema deberá solicitar al usuario cambiar esta contraseña para resguardar la seguridad de cada inicio de sesión. Será responsabilidad del administrador velar porque dicho procedimiento se esté realizando según acuerdo.
- Los privilegios de los sistemas que correspondan a labores administrativas deben ser para usuarios con privilegios en dicha administración y es requerido que el sistema valide este tipo de accesos.
- Cuando un usuario finalice el contrato laboral con la organización, los usuarios, así como los permisos que este maneje, deben ser desactivados y eliminados de forma inmediata, será responsabilidad del encargado que este proceso se dé

correctamente y que la información almacenada quede a cargo del jefe del área para validar el procedimiento a seguir.

- Es responsabilidad del administrador vigilar porque personas externas a la organización no tengan ningún tipo de accesos a las plataformas e información de esta, de haber un caso especial, se debe solicitar la autorización con su justificación por parte de alguno de los mandos altos.
- Es responsabilidad del administrador mantener el control adecuado de la administración del Office 365, incluyendo así, el mantenimiento de las cuentas de correo, la cuenta de almacenamiento en la nube, el servicio de *One Drive* y demás recursos brindados mediante esta plataforma.
- Es responsabilidad del administrador gestionar con recelo, la plataforma de Microsoft Azure y con esto se incluye, todo lo referente a configuraciones del directorio de acceso, servidores, máquinas virtuales y demás recursos que la organización tiene.
- De manejar acceso de terceros en la organización, es requerido crear y firmar entre ambas partes un acuerdo de confidencialidad de la información, dichas firmas deben ser por parte de los altos mandos de las empresas.
- Los administradores, por ningún motivo, deben brindar acceso privilegiado a usuarios que no les corresponda, a excepción de venir la solicitud por parte de los encargados de las áreas, con su debida justificación y tiempo de acceso.
- Es responsabilidad del administrador documentar todo hecho de acto o sospecha de amenaza cibernética, se deben realizar de forma inmediata, las capturas y documentar los eventos relacionados con el hecho; se deberá indicar los procesos o recursos afectados, las áreas de afectación, el tiempo en que fue afectado y las actividades que se realizaron para mitigar dicho proceso. Este tipo de identificación debe estar respaldada en algún lugar seguro, en donde se puede compartir con los usuarios privilegiados del departamento de tecnología.
- Es responsabilidad del Departamento de TI hacer revisiones de, al menos, 1 vez al mes sobre los eventos ocurridos en las diversas plataformas que maneja; además de tener un plan de contingencia ante los eventos que puedan generar algún riesgo importante en la organización.

- Cuando un sistema o equipo opera datos con diversos niveles de sensibilidad, los controles deben ir enfocadas a la protección que se le debe dar a dicha información.
- Es responsabilidad del administrador hacer revisiones de los monitoreos sobre la plataforma Azure, al menos, 1 vez al mes.
- Es necesario garantizar que los servicios de red se encuentren siempre disponibles.
- Es responsabilidad del administrador velar porque el mantenimiento de los equipos, antivirus, bases de datos entre otros recursos, se gestionen de forma constante, según el tiempo que cada recurso requiera.

Organización de la seguridad de la información

Organización interna.

Objetivo. Tratar la seguridad de la información dentro de PRICOSE.

Compromiso de la dirección con la seguridad de la información.

Las altas direcciones deben apoyar la seguridad de la información alojada en la nube de PRICOSE, demostrando compromiso y responsabilidad en la seguridad que se deba establecer dentro de la organización.

Objetivos de control.

Las altas direcciones, en conjunto con el comité de seguridad de la información tienen que:

- Testificar que los fines de la seguridad de la información hospedada en la nube están identificados y que cumplen con las obligaciones de la organización.
- Revisar si la implementación de la política de seguridad se está efectuando según lo acordado.
- Facilitar los recursos necesarios para la seguridad de la información.
- Regularizar dentro de la organización la implementación de los controles de seguridad.
- Generar programas de concienciación hacia el personal, para infundir la importancia del cumplimiento de las políticas de seguridad.
- Dar un apoyo perceptible ante el inicio de la implementación de la seguridad en la organización.
- Aprobar la asignación de roles y responsabilidades específicas para la seguridad dentro de la empresa.
- Es importante que se valide la necesidad de tener alguna asesoría especializada externa para asegurar el mejor rumbo hacia esta implementación, y de ser así,

revisar los resultados obtenidos de la asesoría, con la intención de lograr una prudente toma de decisiones, según el caso analizado.

Coordinación de la seguridad de la información.

Las acciones de la seguridad de la información convendrían estar reguladas por los actores de todas las áreas de la organización con roles y funciones acertadas.

Objetivos de control.

El accionar más responsable que puede tener la organización es que, en este tipo de trabajos, exista una participación por parte de los usuarios, administradores, encargados de áreas y jefaturas; en donde, se pueden hallar habilidades en temas legales, riesgos, recursos humanos y demás, para de esta forma, tener el panorama claro y el camino hacia implementación de una forma exitosa.

La idea de este operar es:

- Aprobar procesos para la seguridad de la información, así como los riesgos y la clasificación de la información.
- Organizar la implementación de los controles de seguridad de la información en la nube.
- Operar de una forma eficiente los planes accionar, ante los incidentes identificados en las revisiones que se realizan.
- Validar la mejor forma en que se puedan identificar la exposición de la información ante las amenazas.
- Avalar que las actividades se realicen en cumplimiento de la política de seguridad.
- Iniciar de una forma eficaz la formación y concienciación de la seguridad de la información en la organización.

El departamento de tecnología deberá asignar algún funcionario como gestor de la seguridad, quien será el responsable de todo lo relacionado con la seguridad de la información, sus funciones se detallarán en esta política.

Si por alguna limitación de la organización, no se puede crear estos grupos con sus funciones separadas, el accionar debe estar a la responsabilidad de la dirección en compañía del encargado del área de tecnología.

Asignación de responsabilidades para la seguridad de la información.

Se definen las responsabilidades en cuanto a la seguridad de la información, de acuerdo con la política de seguridad. Las responsabilidades, de ser necesario, deben integrarse con normas más detallas para sitios o servicios en específico.

Objetivos de control.

Gestor de seguridad de la información.

El gestor de la seguridad de la información debe desenvolver las actividades de coordinación de la seguridad de la información. El departamento de tecnología tendrá a un funcionario que cumpla con esta función tomando las responsabilidades que soporta este rol:

- Exponer, concretar y actualizar políticas, procedimientos y/o normas de la seguridad de la información, junto con el comité de seguridad.
- Crear y mantener actualizado los activos de la información, el gestor deberá tener una metodología para el levantamiento de activos de la información alojada en la nube.
- Valorar y establecer herramientas que mejoren el trabajo de la seguridad de la información.
- Socializar la guía de activos de la información al comité de seguridad y a los participantes de cada área, además de registrar los activos de información.
- Realizar los procedimientos para controlar el acceso a los sistemas de información y a la modificación de los privilegios.
- Valorar, apoyar y generar conceptos técnicos sobre nuevos recursos o plataformas tecnológicas a obtener o implementar en PRICOSE.
- Capacitarse y actualizarse sobre temas de seguridad, nuevas vulnerabilidades y amenazas existentes.
- Crear y revisar los acuerdos de confidencialidad con funcionarios, proveedores y terceras personas que así lo ameriten.
- Promover y apoyar en PRICOSE, la formación en seguridad de la información.

- Lograr asesoramiento de otros organismos o entidades, con el fin de mejorar su gestión, se le permitirá la comunicación con todas las áreas internas de la organización.
- Verificar la aceptación y aprobación de lo identificado y sus planes de tratamiento.
- Revisar al menos una vez al mes los inventarios de activos de información, además de actualizarlos en el momento que surja un cambio del que pueda afectar la seguridad de la organización.
- Definir responsabilidades al grupo de trabajo, sensibilidad y criticidad sobre los activos presentes en la nube de Azure.

Dependencias y departamentos de PRICOSE.

Todos los departamentos de la organización deben tener presente y cumplir los siguientes lineamientos:

- Tener en cuenta los procedimientos y normas de la seguridad de la información en la gestión de la contratación con proveedores y terceros, al igual que en la gestión de cualquier tipo de proyecto.
- Todo requerimiento, problema, suceso o cambio debe ser únicamente reportado y tramitado por el Departamento de TI.
- Las adquisiciones o implementaciones de recursos, solución o plataformas tecnológicas sean hardware o software, deben contar con el visto bueno del Departamento de TI, en compañía del gestor de seguridad de la información, quienes deben valorar las posibilidades técnicas, capacidades, compatibilidad de ser necesario con otros sistemas, integridad, disponibilidad y todo aquello que pueda alterar o poner en riesgo la seguridad de la información.

Asistente Gerencial.

Deberá cumplir las siguientes tareas:

- Es responsabilidad de la o el asistente gerencial de asegurar que los funcionarios, proveedores y terceras personas tengan conciencia de sus responsabilidades, en cuanto a la seguridad de la información y que se dé el cumplimiento de las políticas establecidas por PRICOSE.

- Se asegurará que los funcionarios, proveedores y terceras personas, durante el proceso de selección, comprendan los términos, responsabilidades y condiciones de contratación para lo que se le es contratado.
- La responsabilidad de proteger los intereses de PRICOSE, incorporando un procedimiento ya sea para la terminación o cambio de las responsabilidades del empleo de los funcionarios o del contrato de proveedores y terceras personas.
- Crear un procedimiento formal para la toma de acciones ante cualquier violación a la seguridad de la información que se haya cometido, sean funcionarios, proveedores o terceras personas, dicho procedimiento, deberá tener el visto bueno de la comisión de seguridad de la información, en compañía del gestor de seguridad de la información, para luego divulgarse a los participantes.
- Notificar y divulgar la presente política a todo el personal, así como los cambios que de esta se den, la implementación de la confidencialidad, sobre las actividades de asesoramiento continuo y todo lo que respecta a la seguridad de la información alojada en la nube.
- Será responsable de comunicar al personal que ingresa a laborar a PRICOSE, de sus obligaciones en cuanto al cumplimiento de las políticas, normas y procedimientos de la seguridad de la información.
- Generar los procedimientos ante el cumplimiento de las firmas sobre los acuerdos de confidencialidad de la información definidos por el gestor de seguridad de la información y aprobado por el comité de seguridad de la información, se deberá generar con la manifestación de los conceptos técnicos; una vez aprobado, se incorporará a la demás documentación oficial de PRICOSE.
- Comprender, conocer y aplicar la política de seguridad de la información de PRICOSE en los procedimientos que apliquen a sus labores.

Comisión Legal.

PRICOSE al tener una comisión legal, se delegará las siguientes funciones:

- Es responsabilidad de esta comisión, velar por el cumplimiento de la política de la seguridad de la información en el desarrollo de sus funciones, con sus funcionarios, proveedores y terceras personas.

- Es su responsabilidad asesorar en materia legal a PRICOSE en lo que se refiere a la seguridad de la información.
- Es responsabilidad de esta comisión, requerir la firma del acuerdo de confidencialidad para todo contrato con proveedores, funcionarios que su puesto lo amerite y terceras personas, así como de apoyar la supervisión del cumplimiento de las políticas de seguridad de la información.
- Se concretará un normograma donde se identifique las políticas, normas y recomendaciones emitidas por la Superintendencia General de Seguros (SUGESE) referido a la gestión de las tecnologías de la información que deben establecer sus entidades.

Departamento de Tecnologías de la Información.

- Este departamento tendrá la responsabilidad de dar su concepto técnico, así como el apoyo a los nuevos recursos, instalaciones, soluciones o plataformas tecnológicas tanto en hardware como el software, en donde se valide la posibilidad técnica, compatibilidad y capacidad, integridad, disponibilidad y confidencialidad.
- Deberá resguardar los requerimientos de seguridad de la información, definidos por la administración y comunicación de los sistemas y recursos de tecnología de PRICOSE.
- Los nuevos recursos deben ser aprobados por el departamento de TI, tomando en consideración su uso y el propósito de este, para avalar el cumplimiento de todas las políticas descritas en este documento.
- Tendrá la responsabilidad de restringir el uso de equipos o recursos personales en el lugar de trabajo. Este uso debe ser valorado en cada caso y deber ser autorizado por el departamento de TI en compañía del encargado que corresponda a cada departamento.
- Se debe verificar el hardware y software de los recursos o sistemas adquiridos, para garantizar su compatibilidad con los recursos de otros sistemas que ya se encuentren en producción.
- Comprender y aplicar la política de seguridad de la información de PRICOSE en los procedimientos que apliquen a sus labores.

Proveedores, terceras personas y funcionarios.

- Es responsabilidad de todo funcionario, proveedor o personas externa, llevar a cabo sus labores, testificando de que sus acciones no causen ninguna infracción de seguridad de la información.
- Hacer uso de las mejores prácticas definidas por la organización, en cuanto a la seguridad de la información se refiere.
- Serán los responsables de conocer, dar a conocer y cumplir la política de seguridad de la información vigente de PRICOSE.
- Deberán reportar los acontecimientos de seguridad de la información que se detecten, al gestor de seguridad de la información.
- Es su obligación cumplir con el acuerdo de confidencialidad de la información que se firmó para PRICOSE.
- Notificar al gestor de seguridad de la información, cualquier irregularidad que infrinja contra la seguridad de la información de PRICOSE.
- Comprender, emplear y estar al tanto de la política de seguridad de la información de PRICOSE en los procedimientos que apliquen a su labor.

Propietarios de la información.

Cuando se habla de propietarios, es toda aquella persona responsable de un activo dentro de la organización y cuyas responsabilidades son:

- Efectuar las medidas de seguridad de la información pertinentes en su sitio de trabajo, con el fin de evitar estafas, robos o interrupciones en los servicios de PRICOSE.
- Se asegurará que el personal, proveedores y personas externas tengan las condiciones de confidencialidad en sus contratos y sean consecuentes de sus responsabilidades, lo anterior, a los puestos en que este aplique.
- Definir quiénes, cómo y cuándo se puede tener acceso a la información, según la clasificación interna de la información y la función que este desempeña.
- Notificar al gestor de seguridad de la información sobre cualquier incidente de seguridad, para conocerlo y corregirlo mediante la aplicación de controles ya establecidos.

- Definir si el activo de información está afectando en la protección de los datos y de ser así, aplicar los procedimientos que correspondan según los controles establecidos.
- Comprender, aplicar y conocer la política de seguridad de la información de PRICOSE en las operaciones que apliquen a su labor.

Coordinadores de los sistemas o/y plataformas de TI.

Los coordinadores de los diversos sistemas o bien de las plataformas de TI, deben implementar las políticas, normas, estándares y procedimientos, para resguardar de una forma apropiada la seguridad de la información, dentro de sus funciones se mencionan:

- Emplear los lineamientos de seguridad de la información que le sean informados y que apliquen a su área de administración.
- Evidenciar los aspectos de seguridad de la información aplicados dentro de su área de gestión y su respectivo control de cambios.
- Notificar al gestor de seguridad de la información sobre cualquier incidente de seguridad, para conocerlo y corregirlo mediante la aplicación de controles ya establecidos.
- Comprender, emplear y conocer las políticas de seguridad de la información de PRICOSE en las instrucciones que apliquen a sus labores.

Proveedores, contratistas y/o terceros.

PRICOSE debe instituir para los contratistas, terceros y proveedores, las mismas limitaciones de acceso a la información. Adicionalmente, el acceso a la información debe limitarse a lo mínimo indispensable para efectuar las tareas de las que le fue contratado. Las excepciones deben ser examinadas y aprobadas por el responsable de la información, así como el gestor de seguridad de PRICOSE. Entre las responsabilidades que cada uno de ellos tienen:

- Se deberá firmar un acuerdo de confidencialidad de los datos antes de obtener acceso a la información de PRICOSE
- Las conexiones que se originan desde equipos y redes externas hacia PRICOSE, deben estar limitadas exclusivamente a los servicios y aplicaciones necesarios.

- Cualquier acceso lógico que tenga un proveedor, contratista y terceros, debe ser autorizado por el gestor de seguridad de la información en compañía del coordinador de TI, quienes serán los responsables de las acciones que realice este.
- Es responsabilidad de estos, notificar al gestor de seguridad de la información sobre cualquier incidente de seguridad, para conocerlo y corregirlo mediante la aplicación de controles ya establecidos.
- En el contrato de confidencialidad de la información, se debe definir las obligaciones de seguridad y las acciones a tomar, en caso de una infracción a lo anteriormente firmado.
- Todo proveedor, contratista o personas externa que tenga acceso a los activos de la información en la nube, están en la obligación de cumplir con las políticas de seguridad de información establecidas por PRICOSE.
- Se le dará acceso a la información de los recursos y activos únicamente por medio de una aprobación del propietario del activo de la información y para cuando sea estrictamente necesario.

Cooperación Interinstitucional.

Con el propósito de lograr un asesoramiento para la mejora de las prácticas y controles de seguridad, el gestor de seguridad de la información de PRICOSE, deberá y podrá mantener contacto con entidades especializadas en temas relativos a la seguridad de la información tales como:

Ministerio de ciencia, innovación, tecnológica y telecomunicaciones. (MICITT).
Superintendencia General de Seguros (SUGESE).

- En las actividades de asesoramiento, cuando haya algún intercambio de información de seguridad, es responsabilidad del gestor no exponer o divulgar información confidencial de PRICOSE.
- El intercambio de información confidencial que sean para fines de asesoramiento, únicamente se permite cuando anticipadamente se haya firmado un acuerdo de confidencialidad de la información hacia la entidad requerida y este, debe ser de acatamiento obligatorio hacia todo individuo que participe de los temas comentados.

Proceso de autorización para los servicios de procesamiento de información.

El proceso en donde se autorizan los nuevos servicios o recursos para el procesamiento de la información deben ser autorizados por el gestor de la información en compañía de la comisión de seguridad.

Objetivos de control.

Se tendrán en cuenta las siguientes normas para el proceso de autorización.

- Cuando es necesario, tanto el hardware como el software se deben verificar para asegurar que sean compatibles con otros componentes del sistema, así como la integridad, confidencialidad y disponibilidad requerida, según las políticas anteriormente establecidas.
- La utilización de servicios de procesamiento de información de uso personal, como ordenadores domésticos, laptops, tabletas, móviles, entre otros, podrían estar expuestos amenazas y de esta forma vulnerar la información del negocio, por lo que se deberán identificar, controlar, autorizar y de ser requeridos, implementar controles de seguridad, según las políticas ya establecidas.
- Todo recurso o servicio nuevo debe estar con su autorización y para el usuario conveniente, con su objetivo y su tiempo de uso. Dicha autorización también es necesario que venga del encargado responsable del área a la que pertenece el usuario, con el fin de dar responsabilidad a este, del cumplimiento de las políticas de seguridad de información acordadas.

Acuerdos sobre confidencialidad.

Para los acuerdos de confidencialidad, el gestor de la información y la comisión de TI deberán revisar al menos 1 vez cada 6 meses los requisitos de confidencialidad de la información, a excepción de que exista un cambio que ponga en riesgo la seguridad de la información y que estos acuerdos, tengan que revisarse y adecuarse de forma inmediata.

Objetivos de control.

Los acuerdos de confidencialidad de la información deben abordar las obligaciones a fin de resguardar los datos alojados en la nube, para lo anterior, se recomienda tener en consideración los siguientes puntos:

- Tiempo esperado del acuerdo, tomando en cuenta aquellos casos en que su tiempo debe permanecer de forma indefinida.
- Pertenencia de la información, secretos comerciales, propiedad intelectual y cómo se relaciona con la protección de la información confidencial.
- Procedimientos requeridos cuando se finaliza un acuerdo.
- El derecho de auditar y revisar las tareas que involucran a los datos confidenciales.
- Procedimientos por tomar en cuenta en caso del incumplimiento del contrato.
- Definición de la información que se vaya a proteger (información confidencial)
- Responsabilidades y tareas de los que firman el acuerdo de confidencialidad para impedir la propagación no autorizada de la información.
- El uso permitido de los datos confidenciales y los derechos de los que firman el acuerdo de confidencialidad.
- Cláusulas para la devolución o la destrucción de la información al terminar el acuerdo.
- Procedimientos para la comunicación y el reporte de propagación no autorizada.

Partes externas.

Objetivo. Mantener la seguridad de la información y de los servicios de PRICOSE de los que partes externas tienen acceso o bien, que son dirigidos por estos.

Identificación de los riesgos relacionados con las partes externas.

Se deberán identificar los riesgos que pueden tener la información y los servicios de PRICOSE en donde se involucren partes externas en cuanto a los procesos del negocio.

Objetivos de control.

Ante la necesidad de dar acceso a los servicios y datos de la organización hacia personas ajenas de PRICOSE, se deben considerar una serie de recomendaciones para la identificación de las obligaciones y controles necesarios para poder evaluar el riesgo que esto puede generar a la empresa. Dentro de los puntos a considerar están:

- El tipo de acceso que tendrá la parte externa a la información como ejemplo:

Acceso lógico como base de datos, máquinas virtuales, web *service*, entre otros.

Conexión de red de la organización y la red de la tercera persona, accesos remotos, tiempos de conexión, entre otros.

Tipo de acceso en organización o fuera de ella.

- Los funcionarios de la parte externa involucrados en manejar la información de la organización.
- Medios y controles utilizados por la parte externa para el almacenamiento e intercambio de información.
- Servicios de procesamiento de información que la parte externa necesite del acceso.
- El valor de la información implicada y la importancia que esta tiene para el funcionamiento de las operaciones.
- Los requisitos legales pertinentes a la parte externa que se deben tomar en cuenta.
- Los procedimientos para gestionar los incidentes de seguridad.
- Los controles para resguardar la información que no está contemplada para ser accesible por las partes externas.
- La manera en que se pueden ver afectados los intereses de cualquier otro accionista de la empresa, debido a los acuerdos que se firmaran.
- El impacto del acceso denegado a la parte externa cuando este lo requiera, provocando información inexacta.

Cuando se realiza un acceso a proveedores, contratistas o terceras personas, se deberá, implementar los controles apropiados a cada externo, luego firmar el contrato en donde se refleje los términos y condiciones para la conexión o el acceso. Es importante avalar que la parte externa es consciente de sus responsabilidades y que acepta las obligaciones y deberes implicados en el acceso brindado sobre la información comprometida de PRICOSE.

Gestión de activos

Responsabilidad por los activos.

Objetivo. Identificar y formar responsabilidades de seguridad admisibles para los activos de la organización.

Los activos que se encuentran alojados en la nube deben incluirse y cada uno debe tener un dueño o propietario asignado para el mantenimiento de los controles adecuado según cada activo.

Inventario de los activos.

El inventario de los activos en la organización es el primer mecanismo que se desarrolla para gestionar la seguridad y está compuesta por una lista de recursos ya sean físicos, virtuales, documentación, servicios, instalaciones y demás, que le generen valor a la entidad para resguardarlos ante cualquier riesgo existente. Según lo establecido en las responsabilidades, esta tarea estará a cargo del gestor de seguridad de la información, este es un funcionario del departamento de TI y será el asignado a realizar todo lo referente a los activos que se encuentran alojados en la nube.

Objetivos de control.

Para el caso de PRICOSE, en la tabla se deberá crear la lista de los activos que se encuentran disponibles en la nube de Azure, cada uno de ellos cumplen una función importante dentro de la organización, es por esto, que fue de prioridad realizar la identificación de ellos y de esta forma, empezar a clasificarlos según el nivel correspondiente.

Tabla 7. Guía de Inventario de Activos

Inventario de Activos en la Nube
Departamento de Tecnologías de la Información

# Activo	Nombre de activo	Descripción	Clasificación de activo	Tipo de confidencialidad	Prioridad
PRI-01	Página web	Página web	De servicio	Público	Baja
PRI-02	Hyper-M01	Máquina virtual	Lógicos	Restringido	Alta

Tabla 7. Guía de Inventario de Activos.

Fuente: Elaboración Propia.

Los activos que PRICOSE tiene en su nube según la ISO 27002 se pueden identificar de la siguiente forma:

- Activos de información: en este grupo se encuentran las bases de datos y archivos de datos, cuentas de almacenamiento (respaldos y archivo digital) almacén de claves, contratos, acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación, procedimientos de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoría e información archivada.
- Activos de software: en este grupo entran los diversos softwares que la organización posee.

  Software de aplicación, software del sistema, herramientas de desarrollo y utilidades.
- Activos lógicos: en este caso por tratarse de los activos que se encuentran en la nube, son representados por las máquinas virtuales, discos duros, memorias, servidores.

- Activos de servicios: servicio de comunicaciones, web *services*, *API´s*, servicio de internet, interfaz de red, seguridad de red.
- Activos intangibles. Imagen y reputación de la empresa, habilidades y experiencia de las personas.

Los inventarios de activos de la nube aseguran una protección eficaz de los activos en la organización y también son requeridos por la salud financiera.

Propietario de los activos.

Los activos que se encuentra registrados en el inventario, según ejemplo de la tabla 9, deben contener un propietario referente al tipo de activo, quien se identifica como la persona responsable del control de la producción, del progreso, el mantenimiento, el uso y la seguridad de los activos asignados, el término de propietario, no es dirigido a que dicha persona tenga los derechos de propiedad privado, lo que significa que es el propietario dentro de la empresa, sin embargo, los derechos de este son completamente de PRICOSE.

Objetivos de control.

El gestor de seguridad de la información debe ser responsable de:

- Concretar y revisar al menos una vez cada 3 meses, las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control de acceso.
- Asegurar el buen funcionamiento de los activos.
- Avalar que la información y los activos inscritos con los servicios de procesamiento de la información se clasifiquen de forma adecuada.
- Todas las demás actividades indicadas en la sección de “asignación de responsabilidades para la seguridad de la información” referentes a los activos de la información.
- El gestor de la información puede asignar a una persona para la revisión de este tipo de actividades, sin embargo, la responsabilidad sigue siendo del propietario.

Uso aceptable de los activos.

Es requerido documentar, identificar e implementar reglas sobre el uso aceptable de la información de los activos asociados con los servicios de procesamiento de la información.

Objetivos de control.

Toda persona que tenga un activo de la empresa en su uso deberá regirse bajo las normas señaladas para el manejo de la información de este, con el fin de desempeñar de una manera óptima sus labores diarias; dentro de estas normas se pueden mencionar:

- Es responsabilidad de los empleados, proveedores y terceras personas administrar, mantener y vigilar la seguridad de los activos, para las labores declaradas a su puesto de trabajo.
- No es permitido el uso de los activos con los que cada empleado cuente, para labores distintas a las de su empleo, dentro de la organización.
- En caso de requerir de instalación, actualización o modificación de los activos en la nube, se debe gestionar por medio del encargado del área de TI, de lo contrario, no está autorizado a realizar dicha gestión.
- Además del cumplimiento de las políticas anteriormente establecidas para la seguridad de la información alojada en la nube.

Devolución de los activos.

Tanto los empleados como las partes interesadas externas devolverán todos los activos de la organización en su poder al finalizar su trabajo, contrato o acuerdo.

Objetivos de control.

- La finalización de un contrato o acuerdo debe ultimar legalmente con el retorno de los activos tangibles y electrónicos establecidos anticipadamente que sean propiedad o se hayan confiado a la organización.
- Cuando un trabajador o usuario externo adquiere el equipo de la empresa o utiliza su equipo personal, es significativo seguir los protocolos para avalar que los datos relevantes se trasfieran a la organización y se elimine de forma segura en el equipo.

- En el momento en que un trabajador o usuario externo es consciente de que los datos son requeridos para las operaciones del negocio, debe informarlo y transmitirlo a la organización.
- Se debe vigilar la copia no autorizada de los datos sensibles por parte de los trabajadores y proveedores que cesaron su contrato o acuerdo.

Eliminación de los activos de la organización, en el servicio en la nube.

Los activos de la organización, que están en los locales del proveedor de servicio en la nube, deben eliminarse y de ser necesario devolverse, de una forma pertinente tras el cese del acuerdo del servicio en la nube.

Objetivos de control.

- La organización debe exigir una descripción documentada del cese de los procesos del servicio que contempla la devolución y la eliminación de los activos de la empresa, seguido por la eliminación de las copias de aquellos activos que provienen de los sistemas del proveedor de servicio en la nube.
- La descripción debe nombrar todos los activos y documentar la planificación para el cese del servicio, lo cual deben ocurrir de forma adecuada.
- La organización, de forma planificada y anticipada debe analizar las afectaciones que podrían resultar de este proceso, lo anterior, con el fin de ejecutar los procedimientos necesarios y minimizar cualquier riesgo o afectación en los servicios.

Clasificación de la información.

Se deberá clasificar la información para identificar el valor esperado de protección para el manejo de la información.

Directrices de la clasificación.

La norma ISO 27001 no tiene señalados los niveles con los que se debe clasificar la información, pero deduce que el tipo de clasificación dependerá del grado de importancia que tengan los datos tratados en la empresa ISOTools (2017). El sistema de clasificación de la información apropiado para PRICOSE se debe establecer según

los pilares de la seguridad de la información: de acuerdo con su nivel de confidencialidad, integridad y disponibilidad.

Objetivos de control.

Las clasificaciones y controles de protección referentes a la información deben considerar las necesidades del negocio sobre el compartir o restringir información. Esta actividad está a cargo del gestor de seguridad de la información, en compañía del encargado de TI de ser necesario.

Clasificación según la confidencialidad.

Sobre la información confidencial INCIBE (s, f.) comenta que: "es toda aquella que tenemos que proteger del acceso de otras personas. No importa el soporte, el tipo de información o incluso si se comunica verbalmente". De ello se deduce que estos tipos de datos: son críticos, son sensibles ya que pueden existir otras organizaciones que deseen saberla y, además, hay un compromiso por parte de la empresa en mantener la información de sus clientes como confidenciales.

Con respecto a las características con las que cuenta cada activo, así se distinguirá de su clasificación. Para PRICOSE se establecen tres niveles de acuerdo con la confidencialidad:

- Información de uso restringido: se encuentra disponible específicamente a la(s) persona(s) que se les dio su acceso y que, sin ella, no pudieran cumplir su trabajo. Dichos datos, de ponerse al alcance de las demás personas no autorizadas podrían dejar en riesgo la seguridad, vida o salud de las personas o de la institución (INCIBE, 2019).

- Información de uso interno: los datos de uso interno son aquellos que son accesibles únicamente para el personal de la organización, disponible en cada uno de los departamentos y que, dependiendo de ella, puede ser compartida solo dentro de su misma área (INCIBE, s, f.).

- Información de uso público: se describe como "información que la organización pone a disposición del público dentro de su página web, o que la organización ha hecho pública a través de medios de comunicación" (INCIBE, s, f.). Normalmente este tipo de información se anuncia de forma estratégica para que

la compañía se dé a conocer entre las personas de interés, por lo que no cuenta con ninguna restricción de acceso, sin que esto involucre daños a terceros ni a la misma organización.

Clasificación según la disponibilidad.

La disponibilidad de la información según UNIR (2020) "es un principio fundamental de la seguridad informática que garantiza que la información va a estar disponible para su uso cuando sea requerido" (párr. 10). Para esta clasificación se tomará en cuenta la siguiente categorización:

1. Categoría alta. El no contar con la información, ocasionará, un retraso significativo en los procedimientos y funciones de la organización, un impacto negativo a nivel económico y ante sujetos externos, se podría poner en riesgo la imagen de la empresa
2. Categoría media. El no tener la información a la disposición de la empresa, de igual forma que la categoría alta, puede generar problemáticas en las funciones de la empresa, de nivel económico y de imagen, pero con un riesgo moderado.
3. Categoría baja. En este caso se podría ver afectado la operativa habitual de la empresa, sin embargo, no generaría mayores riesgos a la organización.

Clasificación según la integridad.

ISOTools Excellence (2018) comenta que "La información debe ser verídica, correcta sin alteraciones ni errores". Se consideran los siguientes niveles de integridad:

- Nivel A. Si se genera información alterada, incompleta o con errores, esto ocasionará de forma rígida, un retraso en los procedimientos y funciones de la organización, un impacto negativo a nivel económico y ante sujetos externos, se pone en riesgo la imagen de la empresa.
- Nivel B. Si se genera información alterada, incompleta o con errores, esto ocasionará de forma moderada, un retraso en los procedimientos y funciones de la organización, un impacto negativo a nivel económico y ante sujetos externos, se pone en riesgo la imagen de la empresa.
- Nivel C. En este caso se podría ver afectado la operativa habitual de la empresa, sin embargo, no generaría mayores riesgos a la organización.

Criterios de clasificación.

Con respecto a la clasificación anterior sobre la información, en donde se toma como referencia los pilares de la información, se permite determinar el tipo de activo según su confidencialidad y la prioridad que este represente basándose en el siguiente criterio:

La prioridad es alta cuando el activo tiene como clasificación alta tanto su integridad como su disponibilidad.

La prioridad es media cuando se demuestra que una de sus propiedades (integridad o disponibilidad) se clasifica como alta y la otra como media.

Una prioridad baja se da cuando el activo, en la clasificación de todas las propiedades se determinó como bajo.

Con respecto a los datos de la organización, dentro del inventario de activos según el apéndice 4, se establece una columna en donde se reflejará el tipo de información en que será clasificado ese activo, sea de uso restringido, uso interno o público, así como su prioridad.

Figura 15. Detalle de clasificación de los activos

pricose
SOCIEDAD AGENCIA DE SEGUROS

Inventario de Activos en la Nube
Departamento de Tecnologías de la Información

# Activo	Nombre de activo	Descripción	Clasificación de activo	Tipo de confidencialidad	Prioridad
PRI-01	Página web	Página web	De servicio	Público	Baja
PRI-02	Hyper-M01	Máquina virtual	Lógicos	Restringido	Alta

Confidencial
Restringido
Uso interno
Público

Figura 15. Clasificación de activos.

Fuente: Elaboración propia.

Tomando en cuenta la identificación de los activos y relacionándolo con la clasificación de la información, se pueden distribuir la información de cada activo de la siguiente forma:

- Activos de información. Bases de datos, respaldos, archivo de datos, almacén de claves son de uso restringido, únicamente el encargado del área de tecnología y el gestor de la seguridad de la información pueden manejar dicha información; en el caso de las bases de datos se da autorización a los desarrolladores y de ser necesarios, el encargado dará autorización algún funcionario del área de TI para desarrollar funciones específicas, sin embargo, la responsabilidad será asumida por el encargado.

  Documentación del sistema, manuales de usuario, material de formación, planes para la continuidad del negocio, archivo digital estará clasificada como información de uso interno, tomando las consideraciones que se hayan establecido como políticas para asegurar la información.

  Procedimientos de soporte, acuerdos de recuperación, registros de auditoría e información archivada, serán clasificados como información de uso restringido, solamente por el departamento de TI y según las necesidades y bajo autorización se compartirá con el comité de seguridad de la información y los altos mandos.

- Activos de software. Software de herramientas de desarrollo y utilidades serán clasificados como información de uso restringido, únicamente por el o los desarrolladores, encargado de proyectos, encargado del área de TI y el gestor de seguridad de la información.

  Software de aplicación y del sistema serán de uso interno según los privilegios que tenga cada usuario y con la responsabilidad que se indican en las políticas de seguridad de la información.

- Activos lógicos. Máquinas virtuales. discos duros, memoria, servidores será el encargado del área de TI y el gestor de seguridad quienes tendrán acceso a dicha información, clasificada como de uso restringido.

- Activos de servicios. Servicio de comunicaciones, web *services*, *API´s*, servicio de internet, interfaz de red, seguridad de red, clasificadas como información de uso restringido y los autorizados a trabajar sobre estas serán los desarrolladores, encargado de proyecto, encargado de TI y el gestor de seguridad, bajo las responsabilidades de seguridad de la información anteriormente establecidas.

- Activos intangibles. Imagen, clasificado de uso interno. Ninguna persona externa puede utilizar la imagen de la empresa, a menos de que exista un fin como estrategia de negocio y con la autorización de la gerencia y la junta directiva.

  Reputación de la empresa, habilidades y experiencia de las personas, activos clasificados como uso público.

Etiquetado y manejo de información.

Con respecto al esquema de la clasificación de la información y de los activos de PRICOSE, se debe controlar la forma en la que se etiqueta la información alojada en la nube, dicha actividad estará bajo la responsabilidad del gestor de la seguridad de la información.

Objetivos de control.

En el caso del etiquetado para los activos de PRICOSE alojados en la nube, la plataforma de Azure cuenta con una opción de etiquetado, mediante la cual, se pueden organizar de manera lógica según la clasificación que este tenga.

Las salidas de los sistemas que contienen información clasificada como confidencial tienen que portar una etiqueta de clasificación adecuada, para que se refleje la clasificación, según las reglas establecidas para resguardar la información.

El gestor de seguridad, si así lo desea, puede formar las etiquetas por medio de la herramienta de Azure *Power Shell*. El gestor de seguridad debe apegarse a las responsabilidades y obligaciones que se le asignaron según las políticas anteriormente establecidas.

Control de acceso

Requisitos del negocio para el control del acceso.

Objetivo. Controlar el acceso a la información alojada en la nube. Las reglas del control de acceso deben tener presentes las políticas de la información, anteriormente expuestas.

Política de control de acceso.

Se evidenciará, creará y revisará la política de control de acceso con base en los requisitos de la organización y de la seguridad de acceso.

Objetivos de control.

La política de control de acceso considerara los siguientes parámetros:

- Las normas que existen para la distribución y autorización de la información.
- Las obligaciones que estén relacionadas con la protección del acceso a los recursos o datos de la empresa.
- La distribución de las funciones de acceso como lo son las solicitudes a: creación, autorización y administración de acceso.
- Obligaciones para la revisión de los accesos.
- Los requisitos de seguridad de las aplicaciones individuales del negocio.
- Equilibrio entre el control del acceso y las políticas de clasificación de la información.
- Los perfiles modelo de acceso de usuario para actividades laborales semejantes en la organización.
- Clausura de los derechos de acceso.
- Las pautas que necesitan o no, una aprobación antes de su realización y promulgación.
- Las reglas deben estar basadas en la deducción de lo menos a lo mayormente permitido.

Gestión del acceso de usuarios.

Objetivo. Resguardar el acceso de usuarios que se encuentran permitidos dentro de la organización y aquellos de los que no se debe tener acceso, evitárselos.

Registro de usuarios.

Se establecerá una normativa formal para todo registro y eliminación de usuarios, para permitir o bien rechazar el acceso a los recursos tecnológicos que tiene la organización.

Objetivos de control.

La norma para controlar el registro y la eliminación de usuario contienen:

- Validación de que el grado de acceso concedido, sea el realmente adecuado para cada usuario y según los objetivos de sus funciones, consecuente con la política de seguridad anteriormente se establecida.
- Para admitir que los usuarios se encuentren ligados al acceso correspondiente, se requiere del uso de su ID único, en este caso la identificación, de esta forma se genera responsabilidad hacia los usuarios, sobre las acciones realizadas.
- Se permitirá el uso de identificador (ID) de grupo, cuando las actividades operativas así lo requieran, estos ID deben contar con una aprobación, y se deberán documentar.
- Se debe, eliminar o bloquear de forma inmediata los accesos a todo usuario con cese de su contrato laboral, que haya cambiado sus funciones o bien, renunciado a este.
- Los proveedores del servicio no deben tener el acceso hasta que no se finalicen los procedimientos de autorización, como excepción se dará únicamente acceso al encargado de TI quien es el responsable de realizar las pruebas correspondientes.
- Se debe realizar al menos una vez cada 3 meses, el mantenimiento necesario sobre el registro de los usuarios que tengan accesos, así como velar porque no exista ningún identificador repetido.
- Diferencia entre lo que siempre se debe cumplir a lo temporal.
- Se les brindará a los usuarios una declaración escrita sobre sus derechos de acceso y solicitar la respuesta por parte de ellos, indicando que dar por entendido y aceptado lo escrito en la declaración.

Gestión de privilegios.

Se pretende limitar y vigilar la asignación de privilegios.

Objetivos de control.

Los recursos y sistemas que necesitan de protección contra un acceso no permitido, de vigilar la asignación de los privilegios, por lo que se recomienda tener presenten los siguientes aspectos:

- Se tiene que almacenar un proceso de autorización y registro de los privilegios asignados, en donde se pueda otorgar, hasta que se finalice el procedimiento para la autorización a estos.
- Los privilegios serán asignados a un identificador único (ID), diferente a los que son utilizados para el uso habitual de la organización.
- Se asignarán según la necesidad mínima para su función y de tener opciones especiales, estas serán otorgadas solo cuando sean necesarias.
- Se debe promover el uso de procedimientos del sistema, para impedir el estar otorgando privilegios a los usuarios de manera constante.
- La identificación de los usuarios con sus privilegios asociados hacia cada recurso, sistema y aplicaciones.

Gestión de contraseñas para usuarios.

Se controlará mediante un proceso de gestión, la asignación de contraseñas.

Objetivos de control.

Se recomienda tener en cuenta los siguientes elementos:

- No almacenar contraseñas en sistemas de ordenador en un formato no protegido.
- Se requiere confirmación del recibido de las contraseñas brindadas.
- Formar instrucciones para comprobar la identidad de un usuario antes de generarle una contraseña nueva, de reemplazo o temporal.
- Las contraseñas predeterminadas por el proveedor se deben cambiar, luego de instalar los sistemas.
- Las contraseñas temporales deben ser únicas para un usuario y que no se puedan descifrar fácilmente.

- Requerir a los usuarios la firma de una declaración (agregando términos y condiciones laborales) para conservar las contraseñas de una manera confidencial.
- Las contraseñas temporales deben darse cuando se les crea los accesos a los usuarios e inmediatamente, ellos deben hacer cambio de ella.

Revisión de los derechos de acceso de los usuarios.

Se debe crear un procedimiento formal de revisión cada 3 meses sobre los derechos de acceso de los usuarios.

Objetivos de control.

- Corroborar la asignación de privilegios, para garantizar que no se obtienen privilegios no autorizados.
- Examinar y reasignar los derechos de acceso de usuarios en el momento que haya cambios de un puesto a otro dentro de la misma organización.
- Revisar al menos una vez cada 3 meses, los cambios de privilegios de usuarios y los derechos de acceso.
- Es recomendable revisar las autorizaciones para derechos de acceso privilegiado a intervalos más frecuentes, por ejemplo, cada tres meses.

Responsabilidades de los usuarios.

Objetivo. Prevenir el acceso, robo o exposición de la información y de los recursos de la organización.

Uso de contraseñas.

Las buenas prácticas de seguridad en la elección y uso de contraseñas es lo que se debe pedir a los usuarios, como parte de las responsabilidades asignadas.

Objetivos de control.

Para que se cree un sentido de responsabilidad con el uso de las contraseñas, todos los usuarios se comprometerán a:

- No ingresar contraseñas en registros que son automatizados como las macros.
- No guardar registros de las contraseñas en papeles, archivos entre otros, donde se encuentren a la vista de otros usuarios, a no ser que se guarden con métodos

de almacenamiento seguro y que se encuentren aprobados por el departamento de TI.

- Evitar la reutilización de contraseñas de al menos las últimas 8 veces.
- Cambiar las contraseñas temporales en el primer registro de inicio.
- Amparar la confidencialidad de las contraseñas.
- Evitar la utilización de la misma contraseña para intenciones personales y laborales.
- No compartir las contraseñas que son individuales.
- Realizar el cambio de las contraseñas cuando se indique que exista un riesgo de ella hacia los sistemas y accesos utilizados.
- Acatar las normas adicionales de contraseñas que se encuentran dentro de la política de seguridad de la información.

Equipo de usuario desatendido.

Cada usuario en el momento en que su equipo quede desatendido por el cumplimiento de otras tareas, tiempos de descanso o cualquier otra situación que impida estar al pendiente de este; deberá darle la protección apropiada.

Objetivos de control.

- En el momento en que el equipo no está en uso, protegerlo contra el uso no autorizado por medio del bloqueo de pantalla con clave para volver a su ingreso.
- Cuando se finalice la jornada laboral, finalizar todas las sesiones activas.
- Cerrar por completo los equipos y computadores personales de oficina al terminar la sesión.

Control de acceso a las redes.

Objetivo. Gestionar el acceso a los recursos en red, tanto internos como externos, evitando comprometer la seguridad de la información.

Política de uso de los servicios en red.

El acceso a los recursos que requieran red debe ser exclusivamente a lo autorizado para el usuario.

Objetivos de control.

Las políticas para el uso de las redes deben comprender:

- Las revisiones e instrucciones de gestión para resguardar el acceso a las conexiones de red y los servicios de red.
- Las redes y los recursos de red a los cuales se admite el acceso a los servicios en nube.
- Las condiciones para aprobar el acceso a un proveedor de servicios de Internet o a un sistema remoto.
- Las instrucciones de autorización para establecer a quién se le aprueba el acceso, a qué redes y qué servicios en red.

Autenticación de usuarios para conexiones externas.

El uso de técnicas adecuadas para la autenticación a usuario será lo que permita controlar el acceso de conexiones remotas.

Objetivos de control.

Para la autenticación a conexiones externar se recomienda emplear los siguientes mecanismos:

- Utilización de métodos criptográficos o token de hardware, implementados para soluciones de red privada virtual (VPN)
- Uso de controles de devolución de marcación (control que autentica a los usuarios, formando una conexión con una red de la organización desde sitios remotos por medio de algún modem de retorno de marcación) para brindar protección hacia conexiones no deseadas. Dicho método se debe comprobar totalmente, para determinar que sea una solución apropiada en la organización.
- La autenticación de nodo (método que se utiliza para avalar que el servidor de gestión y los compiladores de datos se comunican de forma segura), cuando se esté conectando a un servicio seguro de equipo compartido, mediante técnicas criptográficas como parte de las soluciones de una VPN.
- Adicional a lo anterior, es importante realizar controles de autenticación para controlar el acceso a las redes inalámbricas.

Protección de los puertos de configuración y diagnóstico remoto.

Se debe vigilar el acceso tanto lógico como físico a los puertos de configuración y de análisis.

Objetivos de control.

Se recomienda tomar a consideración:

- Bloquear mediante una clave y emplear rutinas de soporte para controlar el acceso físico al puerto.
- Garantizar que los puertos de diagnóstico y configuración solo sean viables mediante un acuerdo entre el administrador del servicio del equipo y el personal del soporte que requiere acceso.
- Inhabilitar todo puerto o recurso de los equipos que no son necesarios, para la funcionalidad de estos.

Separación en las redes.

Es necesaria la separación de los grupos de servicios de información, usuarios y sistemas de información.

Objetivos de control.

Dentro de los métodos de control en redes se pueden emplear:

- Dividir en dominios lógicos de red; red internos de la organización y red externos de la organización.
- Efectuar un contorno de red, colocando una puerta de enlace (Gateway) seguro entre las dos redes que se van a interconectar para controlar el acceso y el flujo de información entre los dos dominios, filtrando el tráfico y bloqueando el acceso no autorizado.
- Restringir el acceso a la red utilizando redes privadas virtuales para grupos de usuarios dentro de la organización.
- Los criterios para la separación de las redes en dominios se deben basar en la política de control de acceso.
- De igual forma, se debe tomar en cuenta las políticas de clasificación de la información.

Control de acceso al sistema operativo.

Objetivo. Impedir el acceso no autorizado a los sistemas operativos. Los procedimientos de registro en un sistema operativo están diseñados para disminuir la oportunidad de acceso no autorizado.

Procedimientos de registro de inicio seguro.

Con procedimientos de registro de inicio seguro, se lograr vigilar el acceso a los sistemas operativos.

Objetivos de control.

Para establecer técnicas seguras en los registros de inicio se debe cumplir aspectos como:

- Aceptar la información de registro de inicio, solamente al terminar los datos de entrada. De existir una coincidencia de error, el sistema no debe mostrar cuál parte del dato es incorrecta o correcta.
- No exponer identificadores de aplicación ni de sistema, sin que el registro de inicio esté completado correctamente.
- Publicar un aviso de notificación mostrando que solo tendrán acceso al computador los usuarios autorizados.
- Restringir la cantidad de intentos permitidos de registro de inicio a tres intentos y, además, forzar un tiempo de espera de 5 minutos antes de lograr otro intento, notificar a la consola del sistema si alcanza el máximo de intentos y reconocer intentos correctos e incorrectos.
- No suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado.
- No comunicar claves en texto claro en la red.
- Al momento de generar un registro valido, mostrar los registros fallidos antes del último correcto y la fecha y hora de registro correcto previo.

Identificación y autenticación de usuarios.

Los usuarios deben tener un identificador único (ID) exclusivamente para uso personal y se debe comprobar la identidad de este.

Objetivos de control.

Las revisiones indicadas, deben ser aplicadas hacia todo el personal, sin distinción de tipo de usuario.

- Solo se admiten los ID de usuario genéricos para uso de un usuario, si existen funciones accesibles o si no es necesario rastrear las acciones ejecutadas por el identificador.
- Se permite usar un identificador de usuario compartido para un grupo de usuarios o un trabajo específico.
- Cuando se solicita comprobación de identidad y autenticación, se deben utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, token o medios biométricos.
- Los ID se usarán para rastrear las actividades del responsable.
- El consentimiento por la dirección estará documentado para dichos casos. Se pueden requerir controles adicionales para mantener la responsabilidad.

Sistema de gestión de contraseñas.

La gestión de contraseña se debe dar para resguardar la calidad de las contraseñas.

Objetivos de control.

- Imponer cambios de contraseña.
- Efectuar el uso de identificadores de usuario (ID) individual y de contraseñas para generar compromiso.
- Almacenar un registro de las claves de usuario anteriores y evitar su reutilización.
- No exponer contraseñas en pantalla cuando se registran.
- Asignar una elección de contraseñas de calidad.
- Exigir a los usuarios a cambiar las contraseñas temporales desde el primer inicio.

- Almacenar y transferir las claves en formatos protegidos (encriptadas o codificadas).
- Guardar los archivos de contraseñas de forma dividida de los datos del sistema de aplicación.
- Admitir a los usuarios la elección del cambio de sus contraseñas y que contenga un procedimiento de confirmación para tener en cuenta los errores en los ingresos.
- Verificar que el procedimiento de gestión para distribuir la información de autenticación confidencial, que realiza el prestador de servicio en la nube, satisfaga los requisitos de la organización.

Tiempo de inactivación de la sesión.

Luego de que una sesión se encuentre en un periodo de tiempo de 30 minutos, se establece como inactivo, esta se debe suspender para evitar la infiltración de información.

Objetivos de control.

- El tiempo de inactividad de una sesión debe ser de 30 minutos, una vez sobrepasado dicho tiempo, debe bloquear la pantalla de sesión. La demora con respecto al tiempo en que la sesión se encuentra como inactiva refleja los riesgos de seguridad del área, la clasificación de la información que se maneja y las aplicaciones que se utilizan, así como los riesgos relacionados con los usuarios del equipo.

Limitación del tiempo de conexión.

Se deben contemplar revisiones del tiempo para las aplicaciones sensibles del equipo.

Objetivos de control.

Se tendrá en cuenta:

- La condición en los períodos de enlace para los tiempos normales de oficina (lunes a viernes de 7:00 a.m. a 10:00 p.m.), si no es necesario un tiempo extra u

operaciones de horario prolongado, de esta forma se reduce la oportunidad a un acceso no autorizado.

- Tomar en cuenta el repetir la autenticación en momentos determinados.

Control de acceso a las aplicaciones y a la información.

Objetivo. Impedir el acceso no autorizado a la información que se maneja en los sistemas de aplicación, mediante normas de seguridad para restringir dicho acceso.

Restricción del acceso a la información.

El acceso a las funciones del sistema de aplicación y los datos deben ser restringidos para los usuarios, dicha política debe ser estable

Objetivos de control.

- Examinar los derechos de acceso de otras aplicaciones (leer, escribir, eliminar y ejecutar...).
- Facilitar las opciones para vigilar el acceso a las funciones del sistema de aplicación.
- Avalar que la información de salida de los sistemas de aplicación que manejan información sensible sólo contenga datos oportunos para el uso de la salida y que se envíe exclusivamente a zonas autorizadas; deben tener las revisiones periódicas de dichas salidas garantizando el retiro de la información reiterada.
- Se debe asegurar que el acceso a la información en el servicio en la nube puede ser restringido de acuerdo con la política de control de acceso.
- Restringir el acceso a servicios en la nube, las funciones del servicio en la nube y los datos del cliente mantenidos en el servicio.

Aislamiento de sistemas sensibles.

Hay sistemas de aplicación que requieren un tratamiento especial, debido a su sensibilidad ante la información manejada en ellos.

Objetivos de control.

- Los sistemas de aplicación donde se compartirá recursos y sus riesgos convendrían ser reconocidos y admitidos por el dueño de la aplicación sensible esto, cuando una aplicación se ejecuta en un entorno compartido.

- Se recomienda que se ejecute en un equipo dedicado.
- Exclusivamente se debe compartir recursos con sistemas de aplicación confiables.
- Se identificará y evidenciará la criticidad de un sistema de aplicación por parte del dueño de la aplicación.

Computación móvil y trabajo remoto.

Objetivo. Resguardar la seguridad de los datos, cuando se manejen dispositivos de equipos móviles y de acceso remoto.

Computación y comunicaciones móviles.

Es necesaria la ejecución de normas de seguridad para el amparo contra los riesgos por el uso de los equipos y comunicaciones móviles.

Objetivos de control.

Estas normas deben tomar a consideración:

- Los peligros de trabajar con equipos de computación móvil encontrados en un ambiente sin ninguna protección.
- Realizar copias de respaldo en momentos habituales de la información del negocio. Es recomendable contar con equipo para admitir el respaldo expedito y fácil de los datos. Las copias de respaldo deben tener protección contra robo o pérdida de los datos.
- Prestar atención cuando se manipulan recursos de computación móvil en salas de reuniones, zonas públicas, y demás espacios sin protección fuera de la infraestructura de la organización. Crear la protección para impedir el acceso o la propagación no autorizados de los datos almacenados y procesados.
- Tener cuidado para evadir el riesgo de estar en la mira de personas no autorizadas.
- Agregar las necesidades para el amparo física, las revisiones de acceso, técnicas criptográficas, las copias de respaldo y la protección contra virus.
- Instituir un medio específico en el que se tengan presentes las obligaciones legales, de seguros y otros de seguridad de la organización para los casos de robo o pérdida de los servicios de computación móvil.

- El dispositivo que lleva datos sensibles, importantes del negocio, no deben estar abandonados y deben bloquearse con algún medio físico o usar trinquetes especiales para resguardar el equipo.
- Disponer de la formación del personal que utiliza dispositivos móviles para generar conciencia en los riesgos que se puedan originar, además de las revisiones que se deben efectuar.
- El acceso remoto a los datos, mediante las redes públicas utilizando servicios de computación móvil, únicamente tienen que ejecutarse luego de la identificación y la autenticación del usuario y con los mecanismos adecuados de control del acceso.
- Los servicios de computación móvil deben protegerse de manera física contra robo, fundamentalmente cuando se dejan en sitios no seguros.

Trabajo remoto.

Para las tareas de trabajo remoto de igual forma, se deben implementar normas para asegurar la información que se es manejada.

Objetivos de control.

Se deben considerar los siguientes aspectos:

- El uso de redes domésticas y las prohibiciones en la configuración de servicios de red inalámbrica.
- El ambiente físico de trabajo remoto sugerido.
- Las normas y las instrucciones para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados.
- Contar con dispositivo y medios de almacenamiento para las actividades de trabajo remoto, en donde no se admita el uso de equipo de propiedad privada que no esté bajo el control de la organización.
- Los convenios sobre licencias de software que aprueben a la organización como el responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de los empleados, contratistas o terceras personas.
- Las obligaciones de seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de los datos que se accederán.

- El acceso a equipo de propiedad privada (para verificar la seguridad de la máquina o durante una investigación), el cual puede estar prohibido por la ley.
- Establecer el trabajo que ejecutara la confidencialidad de los datos, las horas laborables y los sistemas y servicios internos con los que el empleado tenga autorización de acceso.

Seguridad de las operaciones

Procedimientos operacionales y responsabilidades.

Objetivo. Resguardar la correcta operación de los recursos de procesamiento de información.

Documentación de los procedimientos de operación.

Se deben documentar y tener a disposición de los usuarios que así lo requieran, las normas de operación.

Objetivos de control.

Se indican las instrucciones para la realización en detalle de cada trabajo, conteniendo de esta manera:

- Copias de respaldo.
- Registros de auditoría y de la información de registro del sistema.
- Guías para el manejo de errores y las restricciones al uso de las utilidades del sistema.
- Administración de la información.
- Ante dificultades técnicas u operativas inesperadas, tener los contactos de soporte necesario.
- Requerimientos de programación, incluyendo las interrelaciones con otros sistemas, hora de comienzo de la tarea inicial y de terminación de la tarea final.
- Procedimientos para el reinicio y la recuperación del sistema que se utilizaran en caso de inconvenientes en el sistema.

Gestión del cambio.

Los cambios en los servicios, los softwares de aplicación y los sistemas operativos deben ser controlados y documentados tomando de referencia el apéndice 9.

Objetivos de control.

- Instrucciones de emergencia, tomando en cuenta las responsabilidades al recuperarse o cancelar los cambios.
- Procedimiento de aprobación formal sobre los cambios propuestos.
- Organización y pruebas de los cambios.
- Valoración de los impactos potenciales de estos cambios.
- Identificación y registro de los cambios significativos.
- Aviso de los cambios a todos los usuarios o personas implicadas.
- Almacenar un registro de auditoria con la información necesaria.
- Tomar en cuenta el impacto de cualquier cambio que deba ser realizado por proveedor del servicio en la nube.

Segregación de funciones.

Al distribuir los sectores de responsabilidad y sus funciones se lograr disminuir las posibles modificaciones que pueden tener los datos, sin previa autorización.

Objetivos de control.

- Es importante mantener el monitoreo de las actividades realizadas.
- Ningún usuario puede tener acceso, cambiar o manejar los activos sin una previa autorización o bien, sin ser descubierto.

Separación de las instalaciones de desarrollo, pruebas y operación.

Al distribuir los sectores de responsabilidad y sus funciones se lograr disminuir las posibles modificaciones que pueden tener los datos, sin previa autorización.

Objetivos de control.

- La información sensible no se copiará en el ambiente de pruebas del sistema.
- El programa de desarrollo y el operativo se ejecutarán en diferentes sistemas y dominios.
- El ambiente en prueba debe emular al ambiente del sistema operativo de la forma más estrecha.
- Cuando no es necesario, no se deben acceder a las herramientas de desarrollo o utilidades del sistema.

- Documentar e indicar las normas de los pases de software del estado de desarrollo al operativo.
- Se deben utilizar perfiles distintos para los sistemas operativos y de pruebas.
- Es vital la separación de los ambientes de desarrollo, producción y pruebas para disminuir el riesgo contra algún cambio accidental o ingresos no autorizados.

Gestión de la prestación del servicio por terceras partes.

Objetivo. Conservar la seguridad de la información y del servicio brindado a terceros.

Documentación de los procedimientos de operación.

Las revisiones de seguridad, las definiciones y niveles de servicio que se indicaron en el convenio deben ser ejecutados y operados por los terceros.

Objetivos de control.

- Incluir los acuerdos sobre la gestión de seguridad para la prestación de servicios externos a la organización.
- Se debe asegurar que las contrataciones a terceros tengan una capacidad suficiente del servicio, en caso de ocurrir algún desastre o fallas significativas.
- Se debe afirmar que la seguridad a la información se mantendrá durante todo el lapso del servicio brindado, en caso de contrataciones externas a la organización.

Monitoreo y revisión de los servicios por terceros.

La revisión y el control de los recursos que serán bridados por las terceras partes, se realizarán regularmente, según la duración del contrato.

Objetivos de control.

- Examinar los reportes del servicio realizado por los externos y agendar sesiones para la revisión del progreso.
- Estudiar los registros y las pruebas de auditoría del tercero en cuanto a los eventos de seguridad, las fallas, las complicaciones operativas, e interrupciones relacionadas con el servicio prestado.
- Solucionar y manipular las dificultades encontradas.

- Proveer datos sobre los sucesos de seguridad de la información, además de analizar esta información por parte de la empresa y de la persona externa.
- Se comprobará el cumplimiento de los acuerdos, monitoreando los niveles de desempeño del servicio.
- La organización debe garantizar que las partes externas asignen responsabilidades para el cumplimiento de lo acordado.
- Se debe tener la claridad sobre las actividades desempeñadas por las partes terceras, así como la gestión de cambios y las vulnerabilidades que se puedan presentar mediante los informes de los registros encontrados.
- La organización definirá los requisitos para el registro de eventos y verificará que el servicio en la nube satisface estos requisitos.
- La entidad debe solicitar información acerca de la sincronización del reloj que se usa para los sistemas del proveedor de servicios en la nube.

Gestión de los cambios en los servicios por terceras partes.

Se gestionará todo lo referente a los cambios en la prestación de los servicios, sea mejoras, nuevos requerimientos y mantenimiento; sin dejar de lado la importancia de los sistemas y métodos del negocio.

Objetivos de control.

La gestión de cambios sobre el servicio contratado debe tener en cuenta:

- Los cambios en los servicios externos para efectuar:
    - Uso de nuevas tecnologías.
    - Aceptación de recursos nuevos o adaptaciones.
    - Cambio de proveedores.
    - Nuevos ambientes de desarrollo.
    - Mejoras o cambios en las redes.
    - Actualización de las infraestructuras de los servicios.

- Los cambios realizados por la entidad para implementar:
    - Alteraciones o reajustes de las normas e instrucciones de la organización.
    - Progresos en los productos ofrecidos actualmente.

- Revisiones para solucionar los acontecimientos de seguridad de los datos.
- Desarrollo de las aplicaciones nuevas.

Planificación y aceptación del sistema.

Objetivo. Disminuir el peligro de las fallas en los sistemas.

Gestión de la capacidad.

Se hará el ajuste y se dará el seguimiento sobre la utilidad de los servicios para certificar el desempeño del sistema.

Objetivos de control.

- Se analizarán los servicios cuya adquisición demanden un costo elevado o bien, tomen mucho tiempo, por lo que es pertinente su monitorización.
- Se identificarán las tendencias en correlación con las herramientas de sistema de datos y de las aplicaciones de la organización.
- Identificar los requerimientos de la capacidad para las actividades ya sean nuevas o existentes.
- Se realizarán controles de investigación para revelar los inconvenientes en el momento adecuado.
- Se debe asegurar que la capacidad acordada y entregada por el servicio en la nube, satisfaga los requisitos de la organización.
- Monitorear el uso de los servicios en la nube y prever las necesidades de capacidad para asegurar el desempeño de los servicios en la nube en el trascurso del tiempo.
- La organización debe estar consciente, en que los recursos entregados por parte del proveedor en la nube pueden tener restricciones de capacidad.

Aceptación del sistema.

Se deben crear criterio de aceptación para los sistemas nuevos, las nuevas versiones y actualizaciones.

Objetivos de control.

Para la aceptación del sistema se deben tener a consideración:

- Certeza de tener en cuenta el resultado del sistema nuevo en la seguridad de la organización
- Elaboración y prueba de instrucciones operativas de rutina para las reglas definidas.
- Exigencias de desempeño y capacidad de los equipos.
- Seguridad que la instalación del nuevo sistema no impresionará desfavorablemente a los sistemas existentes.
- Prácticas para la continuidad del negocio.
- Formación en el uso y empleo de los sistemas nuevos.
- Habilidad de uso, en medida que afecte el desempeño del usuario para impedir el error humano.
- Programaciones de reinicio y de recobro por caídas, y procedimientos de contingencia.

Los altos mandos deben avalar que los requerimientos y los criterios de aceptación de los sistemas son precisos, están documentados y probados.

Protección contra códigos maliciosos y móviles.

Objetivo. Resguardar la integridad del software y de los datos.

Controles contra códigos maliciosos.

Implementación de controles en donde se descubran, prevengan y se recobren los softwares y los datos frente a códigos maliciosos.

Objetivos de control.

- Concretar responsabilidades e instrucciones de gestión a la protección contra códigos maliciosos en los sistemas, su recuperación, la formación de su uso, y los reportes.
- Crear una normar que impida el uso de software no autorizado.
- Ejecución de ordenamientos para comprobar la información concerniente con códigos maliciosos y avalar que los usuarios estén enterados de los inconvenientes de estos códigos y de las falsas alarmas además de saber qué hacer, al recibirlas.

- Revisar de manera regular el software y los datos de los sistemas que dan soporte a los procesos críticos del negocio; se investigara la presencia de archivos no aprobados o alteraciones no permitidas.
- Elaboración de reglas para la continuidad del negocio hacia la recuperación de los ataques de códigos maliciosos.
- Instalación y actualización regular del software de detección y reparación de códigos maliciosos para examinar los equipos y los medios, como revisión preventiva; las comprobaciones realizadas tienen que incluir:
    - Control de las páginas web para evidenciar la presencia de códigos maliciosos.
    - Comprobación de la apariencia de códigos maliciosos en los archivos de medios virtuales o electrónicos y los recibidos por la red, antes de usarlos.
    - Revisión de la aparición de códigos maliciosos en los adjuntos y las descargas del correo electrónico antes del uso.
- Formar una política para el amparo contra los riesgos asociados con la producción de archivos y software, mostrando las medidas de protección que se ejecutaran.
- Ejecución de instrucciones para recoger datos de forma usual, como listados de correo que provean información sobre los códigos maliciosos nuevos o bien, mediante contratos a sitios web de verificación.
- La organización debe solicitar al proveedor de servicio en la nube la información sobre la gestión de las vulnerabilidades técnicas que pueden afectar a los servicios en la nube entregados.
- La organización tendrá que identificar las vulnerabilidades técnicas de sus servicios en la nube y ser responsable de manejar y definir un proceso para manipularlas.

Controles contra códigos móviles.

El código móvil es un código de software que se transporta de un equipo a otro para así, establecerse automáticamente, en donde se puede tener poca o ninguna interacción del usuario. ICONTEC (2007).

La configuración de códigos móviles debe afirmar que se manejan conforme a la política de seguridad de la organización.

Objetivos de control.

Para el amparo contra códigos móviles que realizan acciones no permitidas, se debe tener en consideración:

- Revisión de los recursos utilizables para el ingreso a códigos móviles.
- Bloqueo de la admisión de códigos móviles.
- Realización de los códigos móviles en un ambiente con aislamiento.
- Revisiones criptográficas para legalizar de manera única el código móvil.
- Bloqueo de cualquier uso de códigos móviles.

Respaldo.

Objetivo. Conservar la disponibilidad y la integridad de la información y de los servicios de procesamiento de datos.

Respaldo de la información.

Las copias de respaldos del software y de la información se deben probar con regularidad, en línea con las normas de respaldo convenidas.

Objetivos de control.

Mantener servicios de respaldos puede minimizar el riesgo ante un desastre o falla del software o los datos. Se deben tener presente las siguientes recomendaciones:

- Los respaldos se tienen que resguardar en una distancia lejana, para evitar algún daño ante los desastres que puedan ocurrir en la sede central de PRICOSE.
- Los respaldos se tienen que salvaguardar por medio de encriptación.
- Se debe proporcionar la protección física y ambiental a los datos de los respaldos, que vayan de la mano con las normas aplicadas en la sede principal.
- Se probará con regularidad los medios de respaldo para avalar que sean confiables para el momento en que sean requeridos.
- Hacer registros fieles y completos de las copias de respaldo y crear instrucciones documentadas de restauración.
- Los ordenamientos de restauración se deben evidenciar y probar con regularidad para avalar su eficacia.

- Los respaldos completos, diferenciales e incrementales y la frecuencia de los respaldos deben manifestar las exigencias del negocio, las obligaciones de seguridad de los datos implicados y la importancia del trabajo continuo de la entidad.
- La organización debe solicitar las especificaciones de la capacidad de respaldo de parte del proveedor de servicio en la nube.
- La organización debe verificar que el proveedor de servicio en la nube satisface sus requisitos de respaldos.
- La empresa es la responsable de implementar las capacidades de respaldo cuando el proveedor de servicio en la nube no las entrega.

Registro de acceso y monitoreo.

Objetivo. Reconocer los eventos y generar las evidencias.

Registro de eventos.

Los registros de los sucesos deben originarse, almacenarse y revisarse habitualmente para registrar las actividades de los usuarios, las excepciones, los defectos y los eventos de seguridad de los datos.

Objetivos de control.

Al menos una vez cada quince días, se deben revisar estos eventos y en los registros se deben tomar a consideración los siguientes puntos:

- Tiempos (hora y fecha) y datos de los eventos clave, como inicio y cierre de sesión.
- Identificación del sistema, de la ubicación y terminal cuando sea viable.
- Búsquedas de transacciones en las aplicaciones, elaboradas por los usuarios.
- Intentos de ingreso al sistema con éxito, así como los no permitidos.
- Identificación de usuario.
- Búsquedas de datos logrados y fallidos, así como distintos intentos de acceder a los recursos.
- Cambios en la configuración del sistema.
- Manejo de privilegios.
- Avisos del sistema de gestión de entrada.
- Movimientos del sistema.

- Uso de utilidades de los sistemas, así como su aplicación.
- Los mecanismos de defensa, como los sistemas antivirus y la detección de intrusos, se habilitan y deshabilitan, según sea conveniente.
- Archivos ingresados y sus tipos de acceso.
- Direcciones y protocolos de red.
- Siempre y cuando se utilicen las medidas pertinentes en el campo de privacidad, se pueden registrar los eventos de los datos que son de identificación personal, así como confidencial.
- El encargado de TI será quien revise estos eventos, no debe tener privilegios de eliminar registros de sus propias actividades.
- El encargado de TI, en conjunto de la comisión de seguridad de la información, deberán concretar los requerimientos para el registro de eventos y comprobar que el servicio en la nube satisface estos requisitos.
- El encargado de TI será el responsable de registrar los eventos de las máquinas virtuales y de las aplicaciones que se manejen en la nube.

Protección de la información de bitácora.

El registro y los datos que este contenga estará protegido contra los accesos no permitidos o de cualquier riesgo que pueda darse.

Objetivos de control.

Las revisiones se deben trazar para resguardarlas ante los movimientos no permitidos en los datos del registro y ante inconvenientes operativos, comprendidos:

- Si se excede el área de almacenamiento del medio del archivo de registro, lo que figura que, un evento no está registrado o que los eventos pasados se han sobrescrito.
- Editar o eliminar archivos de registro.
- Variaciones en los tipos de mensajes grabados.
- Se considerará la copia automática a un segundo registro de los tipos de mensajes relevantes o el uso de utilidades de dispositivos o herramientas de auditoría convenientes para efectuar preguntas de archivos y de esta forma, brindar apoyo en clasificar los eventos significativos para el monitoreo de la seguridad de los datos.

- Los registros deben estar protegidos, ante datos que pueden verse como una falsa impresión de seguridad, cuando frecuentemente se modifican o eliminan.
- Para resguardar los registros, se deberá copiar en tiempo real los registros a un sistema fuera del control del operador del sistema.

Bitácoras del administrador y operador.

Las acciones del encargado de TI y del especialista del sistema debe registrarse y estos deben almacenarse de forma segura y monitoreados.

Objetivos de control.

- Es valioso amparar los registros seguros y revisados para avalar que los usuarios privilegiados, sean responsables ante los registros de los medios de procesamiento de datos que son manejados mediante su control.
- Se recomienda manejar un sistema no controlador y administradores de red para monitorear las acciones de cumplimiento del sistema y la administración de la red.
- El encargado de TI con apoyo de la comisión de seguridad de la información determinara si es necesario registrar las capacidades entregadas por el proveedor de servicio en la nube o bien, si el proveedor deberá implementar las capacidades de registro adicional.

Sincronización de reloj.

Los relojes de los sistemas de gestión de los datos relacionados deben componerse en una única fuente de tiempo de referencia para la organización.

Objetivos de control.

- Se solicitará la documentación de las obligaciones de representación del tiempo externamente e internos, sincronización y precisión; pueden ser requisitos de control legal, reglamentarios, contractuales, estandarizados o internos.
- Se concretará un tiempo de referencia estándar para su uso dentro de la organización. Para este caso, deberá ser el tiempo que trabaja la plataforma de Microsoft Azure que es el Tiempo Universal Coordinado (UTC).

- Se documentará e implementara el enfoque de la organización para lograr un tiempo de referencia de una fuente externa y la forma en que los relojes internos se pueden sincronizar de modo confiado.
- Para conservar todos los servidores sincronizados con el reloj experto, se puede manejar un protocolo de tiempo de red.
- El encargado de TI solicitara información acerca de la sincronización del reloj que maneja los sistemas del proveedor en la nube.

Seguimiento de los servicios en la nube.

El encargado de TI debe poseer la capacidad de monitorear aspectos detallados de las acciones de los servicios en la nube que emplea el proveedor.

Objetivos de control.

- El encargado de TI solicitará información al proveedor del servicio en la nube, acerca de las capacidades de seguimiento del sistema disponibles para cada servicio en la nube.
- Se supervisará tanto las aplicaciones como la infraestructura habitada en la nube.
- Se consultarán y analizarán los registros de las actividades y los registros de diagnóstico al menos una vez a la semana.
- Se analizarán las alertas presentes en el servicio en la nube, al menos una vez cada quince días.
- Se configurarán las acciones correctivas que se deben tomar con respecto a las alertas indicadas en el servicio en la nube.

Seguridad de las comunicaciones

Gestión de la seguridad de las redes.

Objetivo. Resguardar la protección de los datos y el amparo de la infraestructura de soporte.

Controles de las redes.

Se deben conservar y controlar las redes con el propósito de asegurarlas contra las amenazas, por lo que se debe tomar en cuenta los siguientes elementos:

Objetivos de control.

- Coordinar las tareas para mejorar el servicio para la organización como para avalar que los controles se aplican en toda la infraestructura del procesamiento de los datos.
- Definir las responsabilidades y las instrucciones para la gestión de los equipos remotos.
- Se debe separar la responsabilidad operativa por las redes de las operaciones del equipo, según la conveniencia.
- Emplear el registro y el monitoreo para consentir el registro de acciones de seguridad.
- Crear revisiones para proteger la confidencialidad y la integridad de los datos que transitan por redes públicas o redes inalámbricas y para el amparo de los sistemas y las aplicaciones conectadas.

Seguridad de los servicios de la red.

Contiene las características de seguridad, los niveles de servicio y los requerimientos de los servicios en la red, indiferente si son servicios que se realizan dentro de la organización o bien, si es un contrato externo.

Objetivos de control.

- Se debe monitorear la capacidad del proveedor de servicio de red para brindar los servicios que se acordaron.
- Identificar las prácticas de seguridad para los servicios ofrecidos por el proveedor.
- Instrucciones para la restricción de accesos a los servicios de red, cuando sea necesario.
- Según las reglas de seguridad, el uso de medidas técnicas para una conexión segura.
- Revisar la autenticación, encriptación y los controles de conexión a la red.
- Se definirán los requisitos para segregar las redes y lograr el aislamiento del proveedor en el entorno compartido de un servicio en la nube.
- Verificar que el proveedor del servicio en la nube cumple y satisface los requisitos para el aislamiento en el ambiente compartido.

Alineación de la gestión de seguridad para las redes virtuales y físicas.

Tras la configuración de las redes virtuales, la estabilidad de las configuraciones entre las redes virtuales y físicas debe basarse en la política de seguridad de red del proveedor del servicio en la nube.

Objetivos de control.

- El proveedor de servicio en la nube deberá concretar y evidenciar una norma de seguridad de los datos para la confirmación de la red virtual consistente con la política de seguridad de los datos para la red física.
- El proveedor debe afirmar que la configuración de red virtual concuerda a la política de seguridad de los datos, independiente de los medios usados para crear la configuración.
- La organización tendrá presenta que, dependiendo del tipo del servicio en la nube, las responsabilidades para configurar una red virtual pueden variar entre la empresa y el proveedor de la nube.

Manejo de los medios.

Objetivo. Impedir la modificación, retiro, propagación o pérdida de los activos no autorizado.

Gestión de los medios removibles.

Se deberán crear los procedimientos para la gestión de los medios removibles.

Objetivos de control.

Se recomienda considerar las siguientes directrices:

- Se debe guardar en un lugar distinto, los datos de los medios que han de estar a disposición por un mayor tiempo, para evadir la pérdida de información por causa de algún deterioro.
- Los dispositivos de medios removibles solo se habilitarán si hay motivos del negocio para hacerlo.
- Se debe requerir autorización para los medios retirados de la organización y almacenar un registro de estos retiros para mantener un control de auditoría.
- Se deben destruir los datos de los medios reutilizables de la organización, cuando estos ya no son indispensables.
- Los medios se deben guardar en un ambiente seguro y custodiado, según las descripciones del fabricante.
- Se debe tomar en cuenta el registro de los medios removibles para impedir la pérdida de datos.

Eliminación de los medios.

La eliminación de los medios se debe realizar de forma segura y evitando cualquier riesgo a la organización.

Objetivos de control.

Tener presenta que, para la eliminación, el riesgo en cuanto a fuga de información debe ser lo mínimo posible, por lo que se recomienda:

- Se debe manejar con recelo, la selección de un contratista apto con revisiones y experiencia sobre la forma de recolección y eliminación de equipo, medios o papel que estos tengan.

- Se guardarán y / o eliminarán de forma segura, aquellos medios que contengan datos sensibles, para impedir su uso; se puede optar por la incineración, trituración o el borrado de datos
- Se mantendrá el registro de la eliminación de los elementos sensibles, con el fin de conservar una prueba de auditoría.
- Se deben establecer instrucciones para identificar los medios que requieren una eliminación segura.

Procedimientos para el manejo de la información.

Las instrucciones para manejar los datos se deben definir con el objetivo de resguardarla contra la propagación ante el uso no autorizado o no debido.

Objetivos de control.

Se deben considerar los siguientes aspectos:

- Rotulado de los duplicados de los medios para la autenticación de la persona autorizada.
- Avalar que la información de entrada está completa y que se emplea la confirmación de la salida.
- Mantenimiento de la comercialización de información en un mínimo.
- Amparo, según el nivel de sensibilidad de la información.
- Prohibiciones de acceso para impedir el acceso de personal no considerado.
- Almacenamiento de los medios según las especificaciones del fabricante.
- Etiquetado de los medios hasta su nivel indicado de clasificación.
- Mantenimiento de un registro formal de los usuarios permitidos.
- Revisión de las listas de distribución y las listas de usuarios autorizados de al menos una vez cada tres meses.

Seguridad de la documentación del sistema.

Se deben proteger los datos del sistema contra los accesos no permitidos.

Objetivos de control.

- La documentación del sistema en la red pública debe mantenerse con los mínimos de privilegios posibles.
- La documentación del sistema se tiene que almacenar con seguridad de la mano con las políticas de seguridad de la información de la organización.
- La lista de acceso a la documentación del sistema se debe proteger como mínima y debe estar considerada por el dueño de la aplicación.

Intercambio de la información.

Objetivo. Conservar la seguridad de la información intercambiada dentro de la organización.

Políticas y procedimientos para el intercambio de información.

Se deberán crear los procedimientos para la gestión de los medios removibles.

Objetivos de control.

En la utilización de servicios para el intercambio de información, se deben tomar en consideración las siguientes pautas:

- Instrucciones para la protección y descubrimiento de códigos maliciosos que pueden ser trasferidos con el uso de comunicaciones electrónicas.
- Ordenamientos para salvaguardar la información electrónica sensible comunicada.
- Directrices que resalten el uso aceptable de los servicios de comunicación electrónica.
- Operaciones para resguardar la información intercambiada contra interceptación, copiado, modificación, enrutamiento inadecuado y destrucción.
- No dejar datos críticos en los dispositivos de impresión como copiadoras e impresoras.
- Instrucciones para el uso de comunicaciones inalámbricas, abarcando los riesgos que puedan darse.

- Inspecciones y limitaciones asociados con el envío de servicios de comunicación, como el envío automático de correo electrónico a direcciones de correo externas.
- Uso de técnicas criptográficas, para la defensa de la confidencialidad, la integridad y la autenticidad de la información.
- Concienciar al personal de no registrar en ningún software, datos como direcciones de cuentas de correo u otra información personal, para impedir que esa información se utilice sin consentimiento.
- En el caso de las llamadas telefónicas o mediante la plataforma Microsoft *Teams*, no revelar información sensible para evitar que, cuando se hace una llamada, sea obstruida u oída por personas que no tienen autorización para escuchar lo comentado.

Acuerdos para el intercambio.

Se deberán crear las normas para el intercambio de información y de software entre la organización y las partes externas.

Objetivos de control.

- Instrucciones para avalar la trazabilidad y el no-repudio.
- Reglas técnicas mínimas para la transferencia de información.
- Posesión y responsabilidades para la protección de la información, derechos de copia, aprobación de las licencias de software, entre otros.
- Compromisos y obligaciones ante sucesos de seguridad de la información.
- Controles especiales que se puedan requerir para proteger los datos sensibles.
- Sistema de etiquetado de los datos críticos, validando que las etiquetas sean comprendidas.
- Responsabilidad de controlar y notificar la transmisión, la comunicación y la recepción.
- Reglas técnicas para incluir y leer la información y el software.
- Normas para identificar los servicios de mensajería.

Mensajería electrónica.

Se debe proteger la información enviada y contenida en la mensajería electrónica.

Objetivos de control.

Las consideraciones para el uso de mensajería deben contener:

- Confiabilidad y disponibilidad del servicio.
- Autenticación que controle el ingreso desde las redes viables al público.
- Avalar que la dirección y el envío del mensaje son los correctos
- Los requisitos para las firmas electrónicas de ser necesario.
- Asentimiento a los servicios públicos externos de mensajería instantánea o el compartido de archivos.
- Resguardar la mensajería contra el ingreso no permitido, la modificación o negación de los servicios.

Adquisición, desarrollo y mantenimiento de sistemas

Requisitos de seguridad de los sistemas de información.

Objetivo. Garantizar la seguridad en los sistemas de la organización antes de su desarrollo o implementación.

Análisis y especificación de los requisitos de seguridad de la información.

Los requerimientos de seguridad deben indicarse para los sistemas nuevos o mejoras en estos.

Objetivos de control.

- Se deben integrar los requerimientos de seguridad para la seguridad de los datos en las etapas iniciales de los proyectos.
- Se abordarán los requisitos de seguridad, cuando existan contratos con terceras personas.
- Se debe mostrar el valor de los activos para la organización, en los requerimientos de seguridad y control.
- Se deben considerar los controles computarizados que se incorporen en el sistema de información, la valoración de los paquetes de software y desarrollos, en los requisitos de seguridad de los datos.
- Cuando se facilita una funcionalidad de mejora adicional y esta cause un riesgo de seguridad, se debe inhabilitar o examinar su estructura de control, para valorar si es conveniente esa mejora disponible.
- Se debe hacer un proceso de adquisición y prueba cuando se obtienen servicios.
- Se deben determinar los requisitos de seguridad de la información para el servicio en la nube.
- Evaluar si los servicios ofrecidos por el proveedor de la nube logran satisfacer los requisitos de seguridad que se desea.
- Se debe solicitar al proveedor de la nube la información sobre las capacidades de seguridad de la información.

Asegurar los servicios de aplicaciones en las redes públicas.

Al poder acceder a la información de las aplicaciones mediante redes públicas, se debe resguardar la información sobre cada aplicación de la organización que debe ingresar el usuario.

Objetivos de control.

- La información de las aplicaciones, que está involucrada en la red pública, debe estar resguardada contra fraude, revelaciones o modificaciones que no se encuentran autorizadas.
- Se deben tomar en cuenta las políticas de uso de la información que se encuentran establecidas en la sección "Políticas de Seguridad de la Información"

Protección de las transacciones de servicios de aplicación.

Se velará por la protección de las transacciones en las aplicaciones.

Objetivos de control.

Para proteger los servicios de aplicación se deben considerar los siguientes puntos:

- Se realizarán validaciones de los datos de entrada a las aplicaciones con el fin de cerciorarse que sean los correctos.
- Se deben realizar instrucciones de respuesta ante errores en la validación de datos.
- Se ejecutarán procedimientos para corroborar la credibilidad de los datos de entrada en las aplicaciones.
- Se deben establecer ordenamientos para impedir que las aplicaciones se ejecuten con un orden erróneo.
- Se controlará la utilización de funciones modificar, borrar y agregar al momento de implementar los cambios en los datos de la aplicación.
- Se vigilará la integridad y autenticidad de los datos descargados entre la aplicación y el equipo de usuario.
- Comprobar que las aplicaciones se ejecuten en el momento correcto.
- Se creará un registro de las actividades realizadas en este proceso.

Seguridad en los procesos de desarrollo y soporte.

Objetivo. Conservar la seguridad del software y de los datos del sistema de aplicaciones.

Política de desarrollo seguro.

Se entiende por desarrollo seguro a la necesidad de tomar en cuenta la seguridad tanto para el diseño como para el desarrollo, desde el minuto cero del ciclo de vida del software, eludiendo de esta forma, inconvenientes de seguridad que representan pérdidas en tiempo, datos, capital y estabilidad del negocio (Ciberseguridad, 2021).

Las medidas para el desarrollo de software y sistemas deben instituirse y emplearse a los desarrollos organizacionales.

Objetivos de control.

Un desarrollo seguro debe incluir la infraestructura, arquitectura, software y sistemas seguros que se desarrollaran. Se deben tomar a consideración los siguientes puntos:

- Las directrices de seguridad para el ciclo de vida del desarrollo del software.
- Se debe asegurar la metodología para el desarrollo del software.
- Se validará la seguridad que se empleará al código para cada lenguaje de programación manejado.
- Se validarán los requerimientos de protección de la fase de diseño.
- Se garantizará los puntos de control de seguridad dentro de los hitos del proyecto.
- Se contemplará la seguridad que se comprenderá en el control de versiones.
- Se debe conocer la capacidad de los desarrolladores para impedir, identificar y corregir las vulnerabilidades.
- La programación segura, se utilizará tanto para el desarrollo de software como para las replicaciones de código en donde los requisitos no están establecidos.
- Los desarrolladores deben estar capacitados y debe validarse el conocimiento para realizar pruebas y revisar código.
- Cuando el desarrollador es contratado, PRICOSE se debe asegurar que el o los desarrolladores cumplen con los principios de desarrollo seguro.
- De ser necesario, PRICOSE debe solicitar al proveedor de la nube, información sobre el uso de procedimientos y prácticas de desarrollo seguro.

Procedimientos de control de cambios del sistema.

Por medio de instrucciones de control, se deben vigilar la implementación de cambios.

Objetivos de control.

- Se documentarán y se harán cumplir las instrucciones de control de cambio con el fin de menguar la infección de los sistemas de información.
- Se deben integrar, cuando sea viable, los procedimientos de control de cambios operativos y de aplicaciones.
- Se deben probar, documentar, especificar y controlar la calidad, cuando exista una apertura de nuevos sistemas.
- Garantizar que la documentación del sistema quede actualizada al terminar cada cambio y que los datos antiguos, según sea necesario, se archivan o eliminan.
- Se avalará que los procesos de control y la seguridad, no se ponga en riesgo por todo acceso brindado a los programadores y los usuarios involucrados.
- Se debe mantener un registro de los niveles de autorización acordados.
- Se deben revisar los controles para no poner en peligro la seguridad de estos cambios.
- Los cambios serán realizados exclusivamente por los usuarios autorizados.
- Avalar que la implementación de los cambios se dé en el tiempo y momento adecuados, sin poner en riesgo ni generar atrasos en la rutina de la organización.
- Se debe aprobar la propuesta antes de iniciar el trabajo.
- Los usuarios autorizados deben aceptar los cambios antes de su implementación.
- Se debe avalar que la documentación operativa y las instrucciones de usuario, se cambian con respecto a la necesidad.

Revisión técnica de las aplicaciones después de realizar cambios de plataforma de operación.

Las aplicaciones de importancia para el negocio (plataforma de administración de cartera de PRICOSE, página principal de PRICOSE, aplicaciones brindadas por el Instituto Nacional de Seguros, plataforma de Office 365, administración de Azure) se deben revisar y probar cuando se realizan cambios de sistemas operativos, para evitar un impacto inesperado en la seguridad.

Objetivos de control.

- Se debe avalar que el plan y el presupuesto anual cubrirán los estudios y pruebas del sistema que resulten de cambios en el sistema operativo.
- Seguridad de que se realicen cambios en los planes de continuidad del negocio
- Se revisarán las programaciones de integridad y control de la aplicación para asegurarse de que no existe ningún peligro debido a los cambios en el sistema operativo.
- Se deben realizar las notificaciones pertinentes con respecto a los cambios en el sistema operativo para consentir las pruebas y revisiones antes de su implementación.

Restricciones sobre los cambios a los paquetes de software.

Las alteraciones a los paquetes de software deben estar restringidas a lo necesario y estos cambios deben contar con un control estricto.

Objetivos de control.

Cuando es requerido modificar los paquetes de software, se deben considerar los siguientes puntos:

- Validar si antes de realizar una modificación, sea necesario obtener el consentimiento del vendedor.
- El riesgo de que los procesos de integridad y de control agregados se puedan ver comprometidos.
- Si como resultados de los cambios, la organización se haga responsable de los mantenimientos futuros, por lo que hay que valorar el impacto que ocurra en ellos.
- La probabilidad de lograr los cambios requeridos del vendedor como un programa estándar de actualizaciones.
- De ser cambios necesarios, el software original se tiene que conservar y los cambios tienen que ser aplicados a una copia.
- Efectuar una gestión de actualizaciones del software para afirmar que los parches y las actualizaciones estén instalados en el programa autorizado.

Ambiente de desarrollo seguro.

En la organización se debe generar un entorno de desarrollo seguro en el cual se incluyen personas, procesos y tecnología en el desarrollo.

Objetivos de control.

Para lograr un desarrollo seguro, se recomienda tener en consideración:

- Evaluar riesgos asociados con el desarrollo de sistemas individuales.
- Se debe revisar el almacenamiento y la transmisión de datos a través del sistema.
- Se velará por la confiabilidad del personal que trabaja en el medio ambiente.
- Se valorará la necesidad de la segregación entre diferentes ambientes para el desarrollo.
- Se controlarán los accesos al ambiente de desarrollo.
- Se controlarán los cambios realizados y el contenido del código.
- Se almacenarán copias seguras fuera del sitio del ambiente de desarrollo.
- Se deben vigilar las transferencias de datos desde y hacia el ambiente de desarrollo.
- Documentar cada actividad sobre este procedimiento.

Desarrollo contratado externamente.

Se debe monitorear y controlar el desarrollo de software que es contratado de forma externa.

Objetivos de control.

Cuando es contratado el desarrollo de software, la organización debe tener en cuenta los siguientes aspectos:

- Los derechos de acceso para controlar la calidad y fidelidad del trabajo contratado.
- Certificación de la calidad y fidelidad del desarrollo contratado.
- Acuerdos sobre licencias, participación de los códigos y derechos de propiedad intelectual.
- Acuerdos de fideicomiso al momento en que, por determinadas razones, la parte contratada no pueda continuar con el proyecto.

- Ejecución de pruebas, antes de la instalación, para descubrir cualquier código malicioso.
- Obligaciones contractuales para la calidad y la funcionalidad de la seguridad del código.

Pruebas de seguridad de sistemas.

Durante el desarrollo, se deben realizar pruebas de funcionalidad de la seguridad de la información.

Objetivos de control.

- Es necesaria una verificación exhaustiva durante los procesos de desarrollo de nuevos sistemas o bien de actualizaciones que se dan en los existentes.
- El alcance del proyecto debe ser proporcional a la relevancia y complejidad del programa.
- Se deben preparar cronogramas detallados de las pruebas a realizar.
- Se deben documentar las pruebas de entrada y los resultados esperados.
- Inicialmente, las pruebas deben ser realizadas por el equipo de desarrollo externo.
- Se deben evaluar comprobaciones específicas para garantizar el funcionamiento del sistema de acuerdo con las expectativas de la organización.

Pruebas de aceptación del sistema.

Las mejoras y los nuevos sistemas deben estar equipados con servicios de pruebas de aceptación.

Objetivos de control.

- Las pruebas de aceptación deben incluir pruebas de seguridad de la información.
- Se deben cumplir las prácticas de desarrollo de sistemas seguros.
- Se deben realizar pruebas de los componentes recibidos y los sistemas integrados.
- Se verificarán las herramientas para el análisis de código.
- Se validarán herramientas para el escáner de vulnerabilidades del sistema.
- Se debe permitir la corrección de defectos relacionados con la seguridad.

- Las pruebas deben ser fiables en el entorno de la organización.

Datos de prueba.

Objetivo. Garantizar la seguridad de los archivos del sistema.

Protección de los datos de prueba.

Se deben proteger y controlar los datos de prueba, a su vez, se deben de elegir de forma cuidadosa.

Objetivos de control.

- Concurrirá una autorización separada cuando se copian los datos operativos en un sistema de aplicación de prueba.
- Los datos operativos se deben quitar del sistema de aplicación de prueba prontamente, después de terminada la prueba.
- Se debe evitar el uso de bases de datos operativos que contengan información sensible con intenciones de pruebas.
- De utilizarse información sensible, todo el contenido debe eliminarse o cambiarse antes del uso, para impedir el reconocimiento de estos datos.
- La utilización de datos operativos se debe registrar para ofrecer un historial para auditoría.
- Las instrucciones de control del acceso que se emplean a los sistemas de aplicación operativos también se deben utilizar en los sistemas de aplicación de pruebas.

Relaciones con los proveedores

Seguridad de la información en las relaciones con proveedores.

Objetivo. Avalar la seguridad de los activos accesibles a los proveedores de la organización.

Política de seguridad de la información para las relaciones con los proveedores.

Los convenios y requisitos de seguridad de la información relacionados con la mitigación del riesgo de acceso de los proveedores a los activos de la organización deben estar documentos y el proveedor debe aceptar dicha alianza.

Objetivos de control.

PRICOSE debe identificar y exigir controles de información de seguridad hacia los proveedores. En los controles se deben incluir los siguientes puntos:

- Modelos mínimos de amparo de la información y procedimiento de acceso para suministrar la base a cada acuerdo con el proveedor con respecto a las necesidades y exigencias comerciales.
- Formación para conocer cómo el personal de la organización se relaciona con el personal del proveedor sobre las medidas adecuadas de colaboración y comportamiento basadas en el tipo de proveedor y el nivel de acceso del proveedor al sistema y a los datos de la organización.
- Técnicas e instrucciones para monitorear el cumplimiento, incluida la valoración de terceros y la confirmación de productos, con modelos definidos de seguridad de los datos para cualquier tipo de proveedor y tipo de acceso.
- Los tipos de obligaciones ajustables a los proveedores para resguardar los datos de la organización.
- Identificación y comunicación reglamentaria de proveedores, como lo son servicios de logística, servicios financieros, los servicios de TI, componentes de infraestructura de TI, que son viables para la entidad.

- Revisiones de la fidelidad e integridad de los datos y la transferencia recibida por cualquier parte para avalar la calidad de la información.
- Manejo de acontecimientos y contingencias de control del cliente, así como las responsabilidades de la compañía y del cliente.
- Resiliencia y procedimientos de recuperación y contingencia para afirmar la disponibilidad por todas las partes de la información o el procesamiento en caso de ser necesario.
- Preparación en la comprensión de las políticas, técnicas y ordenamientos aplicables para el personal de la organización involucrado en adquisiciones.
- Se deben concretar los tipos de acceso a la información permitidos por distintos tipos de proveedores y monitorear y controlar el acceso.
- Documentación sobre la seguridad de la información y las exigencias de control en un acuerdo firmado por ambas partes.
- La organización debe incluir al proveedor de servicio de la nube, como un tipo de proveedor en su política de seguridad de los datos para mitigar los riesgos que se puedan asociar con respecto al acceso que tiene el proveedor del servicio de nube.

Abordar la seguridad dentro de los acuerdos de proveedores.

El proveedor que procese, guarde, observe y comunique información de componentes de infraestructura de TI para la compañía, debe seguir un acuerdo con los requerimientos de seguridad de los datos aplicar.

Objetivos de control.

En la organización se deben concretar los acuerdos con los proveedores, para que ambas partes no malinterpreten las obligaciones de cada uno. Los puntos por incluir en los acuerdos:

- Las exigencias legales, incluidos la protección de datos, los derechos de autor y los derechos de propiedad intelectual, y una descripción de cómo se practicarán.
- Hacer cumplir un plan de revisión acordado, incluidos la gestión de acceso, el análisis de rendimiento, el seguimiento, la presentación de informes y la auditoría para cada parte contratante.

- Representación de la información y las técnicas de acceso a los datos que se facilitará o accederá.
- Normas para el uso aceptable de la información y, de ser preciso, uso inaceptable.
- Detalle claro del personal de los proveedores, autorizado para recibir o acceder a información o procedimientos, condiciones de autorización, y la eliminación, acceso por parte del personal del proveedor de la información de la organización.
- Protocolos específicos y criterios de protección de los datos, tales como respuesta a emergencias, protocolos de autorización, criterios de formación y sensibilización.
- Ordenamientos para la gestión de incidentes.
- Socios comerciales aplicables, como la persona de contacto de TI.
- Los deberes del proveedor de cumplir con los requisitos de seguridad de la organización.
- Descubrimiento de necesidades de los trabajadores del proveedor, comprendidas los compromisos de prueba y notificación, si no se completa la prueba o cuando los resultados dan lugar a dudas.
- Medidas de seguridad de los datos afines a un contrato específico.
- Derecho de auditar los procesos y controles del proveedor contratante.
- La obligación del proveedor de presentar un informe independiente sobre los controles realizados y el convenio de una corrección pertinente en caso necesario.
- El cliente del servicio en la nube debe corroborar los roles y responsabilidades de seguridad de los datos relacionados con el servicio en la nube. Estos pueden incluir los procesos siguientes:
    - Protección contra programas maliciosos.
    - Respaldo.
    - Controles criptográficos.
    - Gestión de la vulnerabilidad.
    - Gestión de incidentes.
    - Revisión del cumplimiento técnico.
    - Pruebas de seguridad.

- Auditoría.
- Colección, mantención y protección de evidencia, incluyendo rastreo de registros y auditorías.
- Protección de la información tras la finalización del acuerdo del servicio.
- Autenticación y control de acceso.
- Gestión de identidad y acceso.

Cadena de suministro de tecnologías de la información y comunicaciones.

Para la atenuación de los riesgos de seguridad de los datos agrupados con los servicios de TI y la cadena de suministro del producto, los proveedores deben tener los acuerdos sobre dichas prácticas.

Objetivos de control.

Para la seguridad de la cadena de suministro, se deben tomar en consideración los siguientes puntos:

- Requerir a los proveedores que divulguen prácticas de seguridad admisibles para bienes de tecnología de la información y la comunicación, si dichos bienes incluyen artículos comprados a otros proveedores.
- Solicitar a los proveedores que comercialicen detalles de seguridad a lo largo de la cadena de suministro para los servicios de tecnologías de la información y la comunicación, si los proveedores subcontratan los servicios de tecnología de la información y las comunicaciones proporcionados a una organización.
- Ejecución de protocolos de ciclo de vida, disponibilidad y riesgos de seguridad relacionados para la gestión de tecnologías de la información y las comunicaciones.
- Ejecución de monitoreo y técnicas de validación apropiados que hayan cumplido con los criterios de seguridad especificados para los productos y servicios de tecnología de la información y las comunicaciones.
- Avalar que los productos se puedan rastrear a lo largo de toda la cadena de suministro y su origen.
- Delimitar los modelos de seguridad de la información para referirse a la creación de productos o servicios de TI.
- Asegurarse que los productos de TI suministrados trabajan como se espera.

- Concretar pautas sobre el intercambio de datos, cualquier inconveniente o compromiso entre organizaciones y proveedores con respecto a la cadena de suministro.

Gestión de la entrega del servicio de los proveedores.

Objetivo. Conservar un nivel de seguridad de los datos y prestación del servicio, según los acuerdos con los proveedores.

Seguimiento y revisión de los servicios de proveedores.

Se debe monitorear, examinar y verificar la prestación de servicios a los proveedores de manera regular.

Objetivos de control.

El seguimiento de los incidentes y problemas relacionados con la seguridad de los datos se realiza con un proceso de gestión del servicio entre PRICOSE y el proveedor:

- Reconocer los aspectos de seguridad de la información de las relaciones del proveedor con sus propios proveedores.
- Revisar los informes de servicio del proveedor y programar reuniones de avance, según lo soliciten los acuerdos.
- Ejecutar auditorías de proveedores y dar seguimiento a los problemas reportados, junto con el análisis de informes de auditores independientes cuando estén disponibles.
- Examinar las huellas de los informes de seguridad de los datos y auditoría del fabricante, dificultades operativas, fallas y seguimiento de fallas con el servicio.
- Monitorear el nivel de desempeño del servicio para comprobar el cumplimiento del acuerdo.
- Proporcionar y revisar los datos con respecto a los sucesos de seguridad según lo dispuesto por los acuerdos y los modelos e instrucciones oportunas.
- Solventar y tramitar cualquier dificultad identificada.

Gestión de cambios en los servicios de proveedores.

Se manejarán los procesos, mantenimiento y mejoras de las políticas de seguridad de los datos, las instrucciones y los controles.

Objetivos de control.

Se tendrán en cuenta los siguientes aspectos:

- Modificaciones de los acuerdos para proveedores.
- Ejecución de cambios por parte de la organización:
    - Mejoras a los servicios brindados existentes.
    - Cambios o modificaciones a las políticas y procedimientos de la organización.
    - Progreso de los nuevos sistemas y aplicaciones.
    - Controles nuevos o actualizados para abordar y mejorar los incidentes de información de seguridad
- Implementar mejoras en los servicios a proveedores:
    - Alteración de la ubicación física del centro de servicios.
    - El uso de la tecnología moderna.
    - Modificación y mejora de la red.
    - Versiones actuales o anteriores con productos existentes.
    - Subcontratar a otro proveedor.
    - Nuevas tecnologías y entornos para el desarrollo.
    - Cambio de proveedor.

Aspectos de seguridad de la información en la gestión de continuidad del negocio

Continuidad de la seguridad de la información.

Objetivo. Efectuar un proceso de gestión de continuidad del negocio para mermar el impacto y la recuperación por la pérdida de activos de la información en la organización.

Planificación de la continuidad de la seguridad de la información.

La organización establecerá los patrones de seguridad de los datos y la relación de su gestión, ante la ocurrencia de situaciones adversas.

Objetivos de control.

- Se fijarán las pautas de seguridad de la información, en la elaboración de la continuidad del negocio y recuperación de desastres.
- La organización valorará, si la continuidad de la seguridad se captura en el proceso de gestión de la continuidad del negocio o en el proceso de recuperación ante desastres.
- Se ejecutará un análisis de efectos comerciales para inconvenientes en la seguridad de la información, para concretar los criterios de seguridad concernientes con condiciones adversas.
- El encargado de TI asumirá que los requerimientos de seguridad de los datos siguen siendo los mismos en condiciones adversas como en condiciones operativas normales, esto sin tener en cuenta un plan de continuidad del negocio.
- Con el fin de disminuir el tiempo de análisis de impacto empresarial, se recomienda capturar los aspectos de seguridad de los datos, dentro de las observaciones de impacto empresarial de gestión de recuperación de catástrofes.

Implementación de la continuidad de la seguridad de la información.

Se limitarán, elaborarán, documentarán y mantendrán procesos, ordenamientos y controles para garantizar la coherencia de seguridad de los datos ante situaciones adversas.

Objetivos de control.

El proceso contendrá los siguientes elementos claves para la gestión de la continuidad del negocio:

- Identificar y considerar la ejecución de revisiones preventivos.
- Avalar la seguridad del personal y el amparo de los bienes de procesamiento de información y de la pertenencia de la organización.
- Percibir los impactos que pueden lograr las dificultades producidas por incidentes de seguridad de los datos (es significativo hallar soluciones para operar los sucesos que originan impactos menores, así como los sucesos graves que alcancen a amenazar la posibilidad de la organización), e instituir los objetivos del negocio para los servicios de procesamiento de los datos.
- Distinguir los riesgos que afronta la organización en términos de la posibilidad y el impacto en el tiempo, conteniendo la identificación y el valor de la prioridad de los procesos críticos del negocio.
- Consideración de la adquisición de pólizas de seguros convenientes y que sean parte del proceso de continuidad del negocio y de la gestión de riesgos operativos.
- Avalar que la gestión de la continuidad del negocio está asociada a los procesos y la distribución de la empresa.
- Caracterización de recursos financieros, organizacionales, técnicos y ambientales suficientes para gestionar los requerimientos identificados de la seguridad de los datos.
- Manifestar y documentar los planes de continuidad del negocio que abordan los requisitos de seguridad de la información acorde con la estrategia acordada d continuidad del negocio.
- Prueba y actualización frecuente de los planes y procesos instituidos.
- Identificar los activos implicados en los métodos críticos de la organización.

Verificar, revisar y evaluar la continuidad de la seguridad de la información.

La continuidad del negocio se debe someter a pruebas y revisiones periódicas para asegurar su actualización y su eficacia.

Objetivos de control.

Las pruebas de la continuidad deben afirmar que todos los involucrados de la recuperación y demás personal oportuno, sean conscientes de los planes y sus responsabilidades para la continuidad del negocio.

Dentro de las técnicas a convenir para dar garantía que las revisiones se encuentren funcionando de forma correcta, se encuentran:

- La continuidad de la infraestructura de los datos, los componentes, las nomas y las revisiones de seguridad de los datos, los métodos y tácticas de gestión de la continuidad del negocio / recuperación de desastres colocan a prueba la calidad y eficacia de la seguridad de la información.
- Practicar y experimentar la confiabilidad de los sistemas, ordenamientos y controles para la protección de los datos, en cumplimiento de los objetivos de continuidad de la información.
- Instruir y probar la experiencia y la rutina en los sistemas, instrucciones y revisiones de la continuidad de la seguridad de los datos para afirmar que su salida esté en línea con los objetivos de la continuidad de la seguridad de la información.

Cumplimiento

Cumplimiento de los requisitos legales y contractuales.

Objetivo. Resguardar contra la violación de obligaciones legales, sistemáticas, regulatorios y contractuales relacionadas con la seguridad de la información.

Identificación de la legislación aplicable y los requisitos contractuales.

Se debe identificar, documentar y actualizar los requisitos legales, reglamentarios y contractuales significativos, en cada uno de los sistemas.

Objetivos de control.

- Los administradores deben mostrarse de acuerdo con la legislación que se encuentra ligada a la organización.
- Debe existir documentación e identificación de los controles básicos y las obligaciones individuales para cumplir con esos criterios.
- En caso de que la organización opere en otros países, los gerentes de cada uno de estos deben avalar el cumplimiento.
- La organización debe considerar que las leyes y reglas oportunas pueden ser aquellas de las autoridades que gobiernan al proveedor de servicios en la nube, además de las que gobiernan a esta.
- Los requisitos legales y regulatorios que se emplean al abastecimiento y al uso de los servicios en la nube deben ser identificados, especialmente, donde las capacidades de procesamiento, almacenamiento y comunicación se distribuyen geográficamente y pueden involucrar múltiples autoridades.
- Los requisitos de cumplimiento legal y contractual son responsabilidad de la organización y no pueden ser transferibles al proveedor de servicio en la nube.

Derechos de propiedad intelectual.

Se implementarán instrucciones adecuadas para salvaguardar el cumplimiento de los requerimientos legales, reglamentarios y contractuales sobre el uso del material en el cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Objetivos de control.

- Obtener software exclusivamente mediante fuentes de confianza para avalar que no se violan los derechos de copia.
- Conservar prueba y certeza sobre la pertenencia de licencias, discos maestros y manuales, entre otros.
- Amparar la concienciación sobre las políticas para resguardar los derechos de propiedad intelectual y comunicar el propósito de tomar acciones rígidas para el personal que los viole.
- No copiar, convertir en otro formato ni extraer de grabaciones comerciales (película, audio) diferentes a los permitidos por la ley de derechos de copia.
- Efectuar revisiones para afirmar que no infrinja el número máximo de usuarios autorizados.
- Conservar registros adecuados de los activos e identificar todos los activos con obligaciones para preservar los derechos de propiedad intelectual.
- No copiar total ni parcialmente libros, artículos, informes ni otros documentos diferentes a los permitidos por la ley de derechos de autor.
- Proveer una política para la colocación o transmisión de software a otros.
- Comprobar que exclusivamente se instalan software autorizado y productos con licencia.
- Facilitar una política para amparar las condiciones de licencia apropiadas.
- Utilizar las herramientas de auditoría convenientes.
- Informar una política de cumplimiento de los derechos de propiedad intelectual que precise el uso legal del software y de los productos de información.
- Cumplir con los términos y condiciones para el software y la información obtenidos de redes públicas.

- La organización debe tener un procedimiento para identificar los requerimientos de licencia específicos de la nube, antes de permitir que se instale cualquier software autorizado en el servicio nube.
- Prestar atención a los casos donde el servicio en la nube es elástico y escalable como en el caso de PRICOSE, el software puede ser ejecutado en más sistemas o núcleos de procesador de lo que es legal en términos de licencia.

Protección de los registros.

Lo registros de la organización se deben resguardar contra destrucción, alteración y pérdida; de acuerdo con las obligaciones legales, reglamentarias, convenidas y del negocio.

Objetivos de control.

- Se tendrá en cuenta la clasificación de la organización, al establecer si se resguardan los documentos organizacionales relevantes.
- Los registros contables, de bases de datos, transacciones, auditoría y operativos, deben contener el detalle sobre los periodos de conservación y el medio autorizado para su almacenamiento, como lo es el papel, microficha, magnético, óptico o virtual.
- Las contraseñas de cifrado coligadas y los programas relacionados con firmas cifradas o digitales se almacenarán para que los registros se descifren en un lapso durante el cual se guardan los registros.
- Se tendrá en cuenta la probabilidad de deterioro de los medios utilizados para el almacenamiento de registros.
- Cuando el tipo de almacenamiento es electrónico, se deben desenvolver protocolos para resguardar contra pérdidas ante posibles cambios técnicos, de esta forma se avala el acceso a la información durante el período de retención.
- Los métodos de almacenamiento de la información, debe fijarse de forma que los datos solicitados logren ser recuperados, dependiendo de las obligaciones por cumplir, en un tiempo y formato aceptable.
- Se proveerán normas con respecto al procesamiento, almacenamiento, administración y eliminación de documentos y datos.

- Se definirá un cronograma para la subsistencia de registros y el tiempo en que deban guardarse.
- Se mantendrá un inventario de las principales fuentes de datos.
- La organización solicitará los datos al proveedor del servicio en la nube, sobre el amparo de los registros almacenados que son acertados al uso de los servicios en esta por parte de la empresa.

Privacidad y protección de los datos personales.

Se avalará el amparo de la información y la privacidad, de acuerdo con la ley y los reglamentos acertados y si se aplica, con las cláusulas del contrato.

Objetivos de control.

- Se desarrollará y efectuará una norma de defensa y privacidad de los datos, esta política se debe comunicar a todas las personas involucradas en el procesamiento de la información personal, dicha política debe regirse bajo la ley sobre la protección de la persona frente al tratamiento de sus datos personales (Ley 8968).
- Es responsabilidad del gestor de seguridad de la información, actuar hacia la protección de los datos personales, para brindar guía a directores, usuarios y proveedores de servicios sobre sus responsabilidades individuales y los ordenamientos específicos que se deban seguir.
- La responsabilidad del manejo de la información personal y de la concienciación sobre los principios de protección de datos deber estar acorde con los reglamentos y la ley correspondiente.

Revisiones de seguridad de la información.

Objetivo. Garantizar que la seguridad de los datos se aplique y gestione de aprobación con las normas e instrucciones de la organización.

Revisiones independientes de la seguridad de la información.

Se debe tener en cuenta internamente las mejoras para la orientación de la organización ante la gestión y cumplimiento de la seguridad de los datos.

Objetivos de control.

- La revisión independiente será revisada por la comisión de seguridad de la información
- Se velará porque la seguridad de la información siga un enfoque coherente, apropiado y eficiente.
- El análisis debe incluir una evaluación de las oportunidades de mejora y de ser conveniente, la necesidad de cambiar el enfoque de seguridad, ya sean políticas y objetivos de control.
- Se deben tener las habilidades y experiencia para desenvolver estas revisiones.
- Las revisiones se deberán registrar e informar a la dirección responsable de iniciar la revisión.
- La organización debe solicitar evidencia documentada de que la ejecución de las revisiones y guía de seguridad de los datos para el servicio en la nube está alineada con cualquier reclamo hecho por el proveedor del servicio en esta.

Cumplimiento con las políticas y normas de seguridad.

La comisión de seguridad debe garantizar que las instrucciones de seguridad dentro las áreas de la organización se llevan a cabo de forma correcta para conseguir el cumplimiento con las políticas de seguridad.

Objetivos de control.

Si del resultado se dio algún incumplimiento, la comisión de seguridad de la información debe:

- Identificar los motivos del incumplimiento.
- Valorar la necesidad de medidas de cumplimiento.
- Efectuar medidas correctivas efectivas.
- Examinar los pasos tomados para verificar su eficiencia y reconocer cualquier deficiencia o vulnerabilidad.
- Los detalles de las evaluaciones y de las medidas disciplinarias deben informarse y documentarse.

Revisiones del cumplimiento técnico.

Los sistemas de información se deben comprobar periódicamente para establecer el cumplimiento con las normas de implementación de la seguridad.

Objetivos de control.

- La comprobación del cumplimiento técnico involucra el examen de los sistemas operativos para asegurar que los controles de hardware y software se han implementado correctamente. Es importante aclarar que este tipo de comprobación del cumplimiento requiere experiencia técnica especializada.
- Si se manejan evaluaciones de vulnerabilidad o pruebas de penetración, se recomienda tener cuidado, pues dichas diligencias pueden poner en riesgo la seguridad del sistema. Estas pruebas se deben planificar, documentar y ser repetibles.
- La verificación del cumplimiento técnico la debe realizar exclusivamente las personas autorizadas y convenientes o bajo supervisión de dichas personas.
- La verificación del cumplimiento técnico se debe realizar ya sea manualmente (con soporte de instrumentos de software apropiadas, si es necesario), por medio de un ingeniero de sistemas con experiencia y / o con la ayuda de herramientas automáticas que crean un informe técnico para la interpretación posterior por parte del especialista técnico.
- Las pruebas de penetración y las evaluaciones de vulnerabilidad suministran una visión instantánea de un sistema en un estado y momento específico. Esta visión se limita a aquellas partes del sistema que se someten a prueba real durante el (los) intento (s) de penetración. Las pruebas de penetración y las evaluaciones de vulnerabilidad no suplantan a la evaluación de riesgos.
- La verificación del cumplimiento también alcanza pruebas de penetración y evaluaciones de la vulnerabilidad, entre otros; dichas verificaciones lo realizan expertos independientes, contratados para este propósito. Ello es ventajoso para descubrir vulnerabilidades en el sistema y comprobar qué tan efectivos son los controles, para impedir el acceso no permitido debido a estas vulnerabilidades.

Relación entre PRICOSE y el proveedor del servicio en la nube

Roles y responsabilidades compartidas dentro de un entorno de computación en la nube.

Objetivo. Esclarecer la relación entre los roles y las responsabilidades compartidas entre la organización y el proveedor del servicio en la nube para la gestión de seguridad de los datos.

Identificación de la legislación aplicable y los requisitos contractuales.

Los compromisos para los roles compartidos de seguridad de los datos en el uso del servicio en la nube deben ser distribuidas a las partes, identificadas, documentadas, comunicadas e implementadas tanto por la organización como por el proveedor del servicio en la nube.

Objetivos de control.

- La organización debe concretar o desarrollar sus normas y procedimientos existentes de acuerdo con el uso de los servicios en la nube.
- Se debe poner al tanto a los usuarios del servicio en la nube de sus roles y responsabilidades en cuanto al uso del servicio en la nube.
- La distribución de los roles y las responsabilidades deben tomar en consideración los datos y las aplicaciones de la organización que protege el proveedor del servicio en la nube.
- Adicional de lo contemplado en la sección “Relaciones con los proveedores”.

REFERENCIAS

Abreu, J. (2012). Hipótesis, Método & Diseño de Investigación. http://www.spentamexico.org/v7-n2/7(2)187-197.pdf

Abreu, J. L. (2014). El método de la investigación Research Method. Daena: International Journal of Good Conscience, 9(3), 195-204.

Aguilar, L. J. (2012). Computación en la nube: Notas para una estrategia española en cloud computing. Revista del Instituto Español de Estudios Estratégicos, (00).

Areitio J. (2008). Seguridad de la información. Redes, informática y sistemas de información de información. Editorial Paraninfo. https://books.google.es/books?hl=es&lr=&id=_z2GcBD3deYC&oi=fnd&pg=IA1&dq=vulnerabilidades+de+la+seguridad+de+la+informacion&ots=wtjkzIJUNm&sig=HQ_PXcpHvs69I5GVhfS0vltffOM#v=onepage&q&f=false

Arias, Á. (2015). Computación en la Nube: 2ª Edición. IT Campus Academy.

Azure (2021). App Service. https://azure.microsoft.com/es-es/services/app-service/#overview

Ciberseguridad (2021). Desarrollo seguro. https://ciberseguridad.com/guias/desarrollo-seguro/#%C2%BFQue_es_el_desarrollo_seguro

Conzultek (s. f). Conozca los tipos de virtualización y sus funciones. https://blog.conzultek.com/productividad/conoce-los-tipos-de-virtualizacion-y-sus-funciones

Conzultek (s. f). Microsoft Azure: qué es, cómo funciona y cómo ayuda en su empresa. https://blog.conzultek.com/microsoft-azure-que-es-como-funciona-como-ayuda-a-las-empresas

Drozhzhin, A. (2020). En qué se diferencian la identificación, la autenticación y la autorización. Kaspersky. https://www.kaspersky.es/blog/identification-authentication-authorization-difference/23914/

Escuela Europea de Excelencia. (2019). Clasificación de la información según ISO 27001. https://www.escuelaeuropeaexcelencia.com/2019/08/clasificacion-de-la-informacion-segun-iso-27001/

Farral, P. (2020). Cumplimiento de estándares y seguridad para proveedores de infraestructura en la nube. https://www.datacenterdynamics.com/es/opinion/cumplimiento-de-est%C3%A1ndares-y-seguridad-para-proveedores-de-infraestructura-en-la-nube/

Fernández Collado, C., Baptista Lucio, P., & Hernández Sampieri, R. (2014). Metodología de la Investigación. Editorial McGraw Hill.

Flores, J. (2021). La norma 27017, comprenderla es una necesidad. https://es.linkedin.com/pulse/la-norma-27017-comprenderla-es-una-necesidad-flores-zepeda

García, C. (2020). Clasificación y tratamiento de la información - ¿Qué es y cómo nos protegemos? https://iveconsultores.com/tratamiento-de-la-informacion/

Garcia, M. A. C. (2019). Fuentes de información. Boletín Científico de las Ciencias Económico Administrativas del ICEA, 8(15), 57-58.

Gaviria, P. (s. f). Seguridad de la información: un tema de tecnología y de conciencia. https://impactotic.co/seguridad-de-la-informacion-educacion-en-toda-la-organizacion/

Goñi Camejo, I. (2000). Algunas reflexiones sobre el concepto de información y sus implicaciones para el desarrollo de las ciencias de la información. Acimed, 8, 201-207.

Hernández Sampieri, R. (2014). Metodología de la Investigación. McGraw-Hill.

Hernández, N. L., & Florez-Fuentes, A. S. (2014). Computación en la nube. Mundo Fesc, 4(8), 46-51.

Ingertec (2020). Controles de seguridad para servicios cloud ISO 27017. https://ingertec.com/ciberseguridad/iso-27017/

Instituto Colombiano de Normas Técnicas y Certificación. (2017). Norma Técnica NTC-ISO/IEC 27002. https://www.vmware.com/latam/solutions/virtualization.html

Instituto Nacional de Ciberseguridad. (2015). ¿A quién dejas acceder a tus sistemas? https://www.incibe.es/protege-tu-empresa/blog/como-pedro-por-su-casa-02

Instituto Nacional de Ciberseguridad. (2019). Primeros pasos para clasificar la información de tu organización. https://www.incibe.es/protege-tu-empresa/blog/primeros-pasos-clasificar-informacion-tu-organizacion

Instituto Nacional de Ciberseguridad. (s, f). La información. https://www.incibe.es/extfrontinteco/img/File/empresas/kit_concienciacion/Pildoras_informativas/incibepresentacin_1__la_informacin__texto.pdf

ISOTools Excellence (2015). SGSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información. https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

ISOTools Excellence (2015). SGSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información. Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

ISOTools Excellence. (2021). Blog calidad y excelencia. ¿Qué son las normas ISO y cuál es su finalidad? https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

ISOTools Excellence. (2021). Blog especializado en Sistemas de Gestión de Seguridad de la Información. ¿Qué es la seguridad de la información y cuántos tipos hay? https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

La universidad en internet. (2020). Disponibilidad en seguridad informática: ¿en qué consiste este término? https://www.unir.net/ingenieria/revista/disponibilidad-seguridad-informatica/

López, P. L. (2004). Población muestra y muestreo. *Punto cero*, *9*(08), 69-74.

Mata Solís, L. (2019). Investigalia. Marco metodológico de investigación. https://investigaliacr.com/investigacion/marco-metodologico-de-investigacion/

Mendoza, S. H., & Avila, D. D. (2020). Técnicas e instrumentos de recolección de datos. *Boletín Científico de las Ciencias Económico Administrativas del ICEA*, *9*(17), 51-53.

Microsoft Azure (s. f). ¿Qué es Azure? https://azure.microsoft.com/es-es/overview/what-is-azure/

Microsoft Docs (2021). Aplicaciones integradas y Azure AD para Microsoft 365 administradores. https://docs.microsoft.com/es-es/microsoft-365/enterprise/integrated-apps-and-azure-ads?view=o365-worldwide

Microsoft Docs (2021). Cambiar la directiva de expiración de las contraseñas de la organización. https://docs.microsoft.com/es-es/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide

Microsoft Docs (2021). Funcionamiento: Azure AD Multi – Factor Authentication. https://docs.microsoft.com/es-es/azure/active-directory/authentication/concept-mfa-howitworks

Microsoft Docs (2021). Instrucciones: Configuración y habilitación de directivas de riesgo. https://docs.microsoft.com/es-es/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-

policies#:~:text=Las%20directivas%20permiten%20excluir%20a,que%20se%20usan%20las%20cuentas.

Ministerio de Trabajo y Seguridad Social (2021). Lista de Salarios Mínimos por ocupación Año 2021. http://www.mtss.go.cr/temas-laborales/salarios/Documentos-Salarios/lista_salarios_2021.pdf

Moreno, E. (2013) Las variables y su operacionalización. https://tesis-investigacion-cientifica.blogspot.com/search?q=variable+instrumental

Orellana López, D. M., & Sánchez Gómez, M. (2006). Técnicas de recolección de datos en entornos virtuales más usadas en la investigación cualitativa.

Organización Internacional de Normalización. (s, f.). Estándares. https://www.iso.org/standards.html

PRICOSE Sociedad Agencia de Seguros (2017). Quiénes Somos https://www.pricose.com/quienes-somos/

Quiroz, S., y Marcías, D. (2017). Seguridad en informática: consideraciones. https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

Red Hat (2021). ¿Qué es la virtualización? https://www.redhat.com/es/topics/virtualization/what-is-virtualization

Rodríguez, R., y Ribón, J. Centro INCA. Políticas de Seguridad Informática PSI. https://www.centroinca.com/centro_inca/documentos/politica_seguridad_informatica.pdf

SecAware (2021). ISO / IEC 27017. https://www.iso27001security.com/html/27017.html

Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica-ESPOL, 28(5).

Tarazona, T., & Cesar, H. (2007). Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología, 28, 137.

Torres, M., Salazar, F. G., & Paz, K. (2019). Métodos de recolección de datos para una investigación.

Universidad del Sur de California (2021). Guías de investigación. https://libguides.usc.edu/writingguide/primarysources

VMware. (2021). Virtualización. https://www.vmware.com/latam/solutions/virtualization.html

APÉNDICES

Apéndice 1. Encuesta

Nombre del Proyecto

Propuesta para la implementación de la seguridad de la información de los servicios en la nube, apoyado en la norma ISO/IEC 27017 para la empresa PRICOSE, Primera Sociedad Agencia de Seguros S.A, ubicado en Guadalupe, San José.

Nombre de la Sustentante

Karla Araya Rivera

Objetivo del instrumento y público meta

Comprender el conocimiento que tiene el personal de la organización hacia la seguridad de la información y del manejo de los activos que se les han sido asignados. La encuesta será aplicada a los empleados directos de la organización.

Preguntas por realizar

1. Seleccione su rango de edad.

De 18 a 30 años

De 31 a 50 años

Mayor de 50 años

2. Seleccione su género.

Femenino

Masculino

Otro

3. Seleccione su departamento.

Operaciones

Administrativo

No estoy seguro

4. ¿Conoce y entiende el término de seguridad de la información?

Sí

No

No estoy seguro

5. ¿Es capaz de identificar un virus o posible ataque en su equipo portátil?

Sí

No

No estoy seguro

6. ¿Conoce los riesgos del uso de redes wifi-públicas?

Sí

No

No estoy seguro

7. ¿Cuenta con la capacitación adecuada por parte de la empresa para la prevención de los riesgos en la seguridad de la información?

Sí

No

Lo desconozco

8. Al momento de ingresar a los sistemas de la empresa, ¿cuenta con un usuario y contraseña **única** que permite dicho acceso?

Sí

No

Lo desconozco

9. Para el acceso a su cuenta de correo, Microsof Teams y One Drive, ¿Tiene el doble factor de autenticación habilitado? (doble clave de seguridad).

Sí

No

Lo desconozco

10. ¿Hace uso adecuado de las contraseñas que tiene en cada sistema que ejecuta?

Sí

No

No estoy seguro

11. ¿La empresa tiene personal responsable de velar por la seguridad de la información?

Sí

No

Lo desconozco

12. ¿La empresa cuenta con políticas que especifican el detalle de sus funciones desempeñadas?

Sí

No

No estoy seguro

13. ¿PRICOSE dispone de normas sobre el uso de los activos tecnológicos con los que usted trabaja (equipo portátil, monitores, teléfonos móviles, entre otros)?

Sí

No

No estoy seguro

14. ¿La empresa cuenta con normas establecidas para el uso adecuado de los datos con la que usted trabaja?

Sí

No

Lo desconozco

15. De existir estas políticas, ¿fueron notificadas formalmente y aceptadas por usted?

Sí

No

No estoy seguro

Apéndice 2. Entrevista

Nombre del Proyecto

Propuesta para la implementación de la seguridad de la información de los servicios en la nube, apoyado en la norma ISO/IEC 27017 para la empresa PRICOSE, Primera Sociedad Agencia de Seguros S.A, ubicado en Guadalupe, San Jose.

Nombre de la Sustentante

Karla Araya Rivera

Objetivo del instrumento y público meta

Identificar los procesos que se realizan para proteger la información que se encuentra alojada en la nube. La entrevista va dirigida al coordinador del departamento de TI.

Preguntas por realizar

1. ¿Tiene control de la seguridad de todos los usuarios de la empresa?
2. ¿Se cuenta con un plan de prevención de riesgos informáticos?
3. ¿La empresa tiene documentación formal sobre la clasificación de la información?
4. ¿Conoce en su totalidad, cuáles son los servicios de la empresa que se encuentran hospedados en la nube?
5. ¿Se hace revisiones periódicas sobre las copias de seguridad de los datos que se encuentran automatizadas en la nube?
6. Según el perfil de cada usuario, ¿se manejan políticas de restricciones para el uso de los datos?
7. ¿Se encuentran los sitios web de la organización protegidos?
8. ¿Existe forma de conocer cuáles son los equipos que generan mayores amenazas en su organización?

9. Con respecto al servicio de nube contratada, ¿conoce cómo gestiona su proveedor los riesgos de seguridad de la información?
10. ¿Tiene claro, cuáles son las tareas de seguridad que le competen al proveedor y cuáles son las que debe realizar el departamento de informática?
11. ¿Conoce a cuáles datos se les realizan respaldos de seguridad y a donde se encuentran alojados?
12. Si el proveedor de la nube tuviese algún inconveniente administrativo o legal, ¿sabe cuáles son las garantías de seguridad de los datos que el proveedor le brindará?
13. ¿Utiliza las alertas y reportes de los eventos disponibles que se tiene con el servicio contratado en la nube?
14. ¿La empresa cuenta con políticas para gestionar y regular la eliminación de los activos?
15. ¿Existen procedimientos documentados para gestionar los perfiles y permisos de usuarios para el acceso a los sistemas hospedados en la nube?
16. Al momento de ocurrir una renuncia o despido, ¿se gestiona la eliminación y des habilitación de usuarios de forma expedita?
17. ¿Se manejan procedimientos formales al momento de ocurrir algún evento que exija a realizar cambios de contraseña, perfiles o permisos?
18. ¿Se inspecciona de forma habitual los derechos de acceso con los que cuenta cada usuario, incluyendo los que tienen accesos más privilegiados?

Apéndice 3. Observación

Nombre del Proyecto

Propuesta para la implementación de la seguridad de la información de los servicios en la nube, apoyado en la norma ISO/IEC 27017 para la empresa PRICOSE, Primera Sociedad Agencia de Seguros S.A, ubicado en Guadalupe, San Jose.

Nombre de la Sustentante

Karla Araya Rivera

Objetivo del instrumento y público meta

Identificar las amenazas presentes de los servicios e información hospedadas en la nube. Este instrumento se basará específicamente en lo observado dentro de la plataforma de Microsoft Azure.

Bitácora de Observación				
Fecha de Observación:				
# Observación	**Herramienta observada**	**Detalle de observación**	**Resultado obtenido**	**Tiempo de ejecución**

Apéndice 4. Inventario de los activos en la nube.

Inventario de Activos en la Nube
Departamento de Tecnologías de la Información

# Activo	Nombre de activo	Descripción	Clasificación de activo	Tipo de confiden-cialidad	Prioridad
PRI-01	Página web	Página web	De servicio	Público	Baja
PRI-02	Hyper-M01	Máquina virtual	Lógicos	Restringido	Alta

Apéndice 5. Cuadro de aprobación de las políticas de seguridad de la información.

Aprobación de las Políticas de Seguridad de la Información

ID Política	Rol	Nombre	Fecha de aprobación	Cargo Desempeñado	Firma

Apéndice 6. Comisión de seguridad de la información.

Pricose Primera Sociedad Agencia de Seguros S.A.
Comisión de Seguridad de la Información | Período:
Aprobada en Sesión Junta Directiva N°. XX

Rol	Primera Apellido	Segundo Apellido	Nombre	Representación en la compañía

Apéndice 7. Control de cambios en las políticas de seguridad de la información.

Pricose Primera Sociedad Agencia de Seguros S.A.
Control de cambios en las políticas de la seguridad de la información

Versión modificada	Fecha de revisión	Motivo de actualización	Responsable del cambio	Firma

Apéndice 8. Control de versión.

Pricose Primera Sociedad Agencia de Seguros S.A.

Control de versión en las Políticas de la Seguridad de la Información en la nube

Versión	Fecha	Realizado por	Detalle	Firma
V-1.0				

Apéndice 9. Bitácora de cambios en servicios, softwares y sistemas.

Pricose Primera Sociedad Agencia de Seguros S.A. **Bitácora de cambios en servicios, software y sistemas**							
Información del proceso							
Nombre del proceso:							
Encargado:							
# Cambio	**Descripción del cambio**	**Prioridad**	**Fecha de solicitud**	**Solicitado por**	**Estado**	**Fecha de resolución**	**Notas**