FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27002:2013, SECCIÓN "CONTROL DE ACCESO" PARA LAS APLICACIONES INFORMÁTICAS DE LA ASEGURADORA DEL SUR.

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de

TECNÓLOGO EN REDES Y TELECOMUNICACIONES

Profesor Guía

ING. KARINA TERÁN

Autor

ROBERTO ERMEL HUACANÉS CHÁVEZ

Año

2016

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

Karina Maribel Terán Valenzuela

Ingeniera

1712627114

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

ROBERTO ERMEL HUACANÉS CHÁVEZ

1714736319

AGRADECIMIENTO

Agradezco a mis padres por su incesante apoyo para concluir esta etapa, a mis hermanas por su ejemplo de tenacidad y constancia, a mi esposa por su paciencia y a mi adorada hija por ser la inspiración para continuar.

DEDICATORIA

Dedico este trabajo a todos aquellos que, con su apoyo, hicieron posible la culminación del mismo; y a la UDLA que me brindó la oportunidad de alcanzar esta valiosa meta.

RESUMEN

La presente tesis da a conocer la estructura del estándar ISO/IEC 27002:2013, sección “Control de acceso a los sistemas y aplicaciones” informáticas; citando conceptos fundamentales para la comprensión y elaboración de políticas de seguridad. Analiza el estado actual del acceso a las aplicaciones en la Aseguradora del Sur y propone directivas que darán inicio al establecimiento de las mejores prácticas basadas en el mencionado estándar.

Por último, se hace recomendaciones que buscan apoyar la gestión de Seguridad de la Información para minimizar los riesgos relacionados con el acceso a información confidencial de la compañía y ayudarán a fortalecer la imagen institucional de la Aseguradora del Sur.

ABSTRACT

This thesis aims to make know the structure of ISO/IEC 27002:2013 standard, section informatics “System and application access control”, mentioning fundamental concepts for the understanding and development of security policies. Analyzes the current state to access to applications in the Aseguradora del Sur and proposes directives that will begin the establishment of best practices based on the above mentioned standard practices.

Finally, makes recommendations intended to support the management of information security to minimize risks related to access to company´s confidential information and will help strengthen the institutional image of the Aseguradora del Sur.

Indice

CAPÍTULO I: FUNDAMENTACIÓN DE LA IMPORTANCIA DE REGULARIZAR EL ACCESO DE LOS USUARIOS A LA INFORMACIÓN DE LA EMPRESA 1

1.1 EL ESTÁNDAR ISO/IEC 27002:2013 1

1.2 DEFINICIÓN DE INFORMACIÓN, SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN. 3

1.2.1 Información 4

1.2.2 Seguridad informática y Seguridad de la información 5

1.2.3 Requerimientos de seguridad de la información. 6

1.2.4 Impacto en la organización 7

1.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN (PSI) 7

1.3.1 Elementos de una PSI 8

1.3.2 Parámetros para establecer PSI 9

1.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES 11

1.4.1 Restricción de acceso a la información 11

1.4.2 Procedimientos seguros de inicio de sesión 12

1.4.3 Sistema de gestión de contraseñas 13

1.4.4 Uso de programas de utilidad privilegiados 14

1.4.5 Control de acceso al código fuente de los programas 15

CAPÍTULO II: ANÁLISIS DEL ESTADO ACTUAL Y LA FACTIBILIDAD DE LA IMPLEMENTACIÓN DE UNA NORMA INTERNACIONAL DE ACCESO..... 17

2.1 MARCO METODOLÓGICO 17

2.2 ANÁLISIS DE ACCESO ACTUAL A LAS APLICACIONES INFORMÁTICAS DE LA ASEGURADORA DEL SUR 18

2.2.1 Aplicaciones analizadas..... 18

2.2.2 Análisis FODA..... 20

2.2.3 Reseña histórica de la empresa 21

2.2.4 Organigrama de la empresa 22

2.3 ANÁLISIS DE FACTIBILIDAD DE IMPLEMENTACIÓN DE LAS MEJORES PRÁCTICAS DE CONTROL DE ACCESO. 23

2.3.1 Análisis de la información 23

2.3.2 Aplicaciones informáticas de la aseguradora del sur factibles a implementar el estándar ISO/IEC 27002:2013 24

CAPÍTULO III: IMPLEMENTACIÓN DEL ESTÁNDAR ISO/IEC 27002:2013SECCIÓN “CONTROL DE ACCESO A LOS SISTEMAS Y APLICACIONES” 26

3.1 MANUAL DE SEGURIDAD DE LA INFORMACIÓN, SECCIÓN CONTROL DE ACCESO A LOS SISTEMAS Y APLICACIONES. 26

3.2 PROPUESTA DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 26

3.3 PROPUESTA DE PROCEDIMIENTOS PARA CONTROL DE ACCESO A LAS APLICACIONES 28

3.3.1 Restricción de acceso a la información 28

3.3.2 Procedimientos seguros de inicio de sesión. 32

3.3.3 Sistema de gestión de contraseñas: 33

3.3.4 Uso de programas de utilidad privilegiados 34

3.3.5 Control de acceso al código fuente de los programas 35

IV. CONCLUSIONES 35

V. RECOMENDACIONES 36

GLOSARIO DE TÉRMINOS: 38

Referencias 41

ANEXOS 42

CAPÍTULO I: FUNDAMENTACIÓN DE LA IMPORTANCIA DE REGULARIZAR EL ACCESO DE LOS USUARIOS A LA INFORMACIÓN DE LA EMPRESA

1.1 EL ESTÁNDAR ISO/IEC 27002:2013

Como estándar internacional, ISO/IEC.27002 es ampliamente difundido y aplicado. Se trata de un estándar para la seguridad de la información que tiene su origen en 1995, publicado como BS 7799-1. A partir de este, se generaron revisiones posteriores que cito a continuación:

- BS-7799-1 (1999). Se trata de un código de buenas prácticas de seguridad de la información y describe los elementos clave que permiten asegurar una implementación efectiva de la seguridad.
- BS 7799-2 (1999). Especifica los requisitos que permiten establecer, implementar y documentar un sistema de gestión de la seguridad (SMS) y forma la base para la valoración del sistema de gestión de la seguridad de la información.

Los procesos y actividades que integran la gestión de la seguridad de la información según ISO-17799 son el desarrollo de una política de seguridad de la información, la identificación de funciones y responsabilidades dentro de la organización, el análisis y gestión de vulnerabilidades, impactos, riesgos, salvaguardias, riesgos residuales y limitaciones. Asimismo, incluye la gestión de la configuración, la gestión de cambios, la planificación de contingencias y de recuperación ante desastres, la concienciación y formación de la seguridad y el seguimiento. El seguimiento incluye

mantenimiento, auditoría de seguridad, verificación, revisión continua y gestión de incidentes. (Arteitio, 2008).

En el año 2000, ISO/IEC publicó la versión revisada con el título “Information technology – Security techniques – Code of practice for information security management”. Posteriormente, tras otra revisión en 2005, se publicó el documento modificado ISO/IEC 17799:2005.

Finalmente, en el año 2007, con la reserva de la numeración 27000 para la Seguridad de la Información, el estándar pasó a llamarse ISO/IEC 27002.

Este estándar no es una norma de certificación ni fue diseñada para ese propósito. Se trata de un: “…Código de buenas prácticas para un Sistema de Gestión de la Seguridad de la Información (SGSI), la cual como lo indica en su título ofrece recomendaciones para la gestión de un SGSI. (Instituto Uruguayo de Normas Técnicas, 2014)”

En cuanto a su estructura, según el estándar ISO/IEC-27002:2013, “se compone de 14 dominios, 35 objetivos de control y 114 controles (Instituto Uruguayo de Normas Técnicas, 2014).”Si bien cada actualización del estándar puede re organizar los dominios y secciones, para este caso, lo más relevante sería mencionar que, (Gutierrez, 2013)lo relacionado con dispositivos móviles y teletrabajo que antes estaba asociado al Control de Accesos, ahora se encuentra dentro de la sección 6: Organización de la Seguridad de la Información. Y dentro de la sección de Control de Accesos se engloba lo relacionado con acceso al sistema operativo, a las aplicaciones y la información.

Figura 1. Diagrama explicativo del estándar ISO/IEC-27002:2013.
Tomado de http://www.iso27000.es

La implementación de una política de seguridad de la información basada en el estándar ISO 27002:2013, permite a las Organizaciones:

- Gestionar de manera efectiva los recursos de información críticos,
- Instalar y administrar los mecanismos de protección adecuados,
- Determinar qué conductas son permitidas y cuáles no.

Al ejecutar estas actividades, se logra una efectiva reducción de los niveles de riesgo y de las vulnerabilidades que se traduce en ahorro de tiempo y dinero, genera mayor confianza organizacional y logra un fortalecimiento de la imagen institucional; al mismo tiempo que mejora la competitividad en el mercado.

1.2 DEFINICIÓN DE INFORMACIÓN, SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN.

1.2.1 Información

Información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

“La información debe considerarse un activo importante con el que cuentan las Organizaciones para satisfacer sus objetivos, razón por la cual, tiene un alto valor para las mismas y es crítica para su desempeño y subsistencia. (ARCERT, Manual de Seguridad en Redes, 2013)”

Vulnerabilidades y Amenazas de la información

“Una vulnerabilidad es una debilidad en un activo. Una amenaza es una violación potencial de la seguridad. No es necesario que la violación ocurra para que la amenaza exista. Las amenazas “explotan” vulnerabilidades (ARCERT, Manual del Instructor de Seguridad, 2013)”

Actualmente, las amenazas informáticas pueden dividirse en Naturales y Humanas. A continuación se muestra un cuadro donde puede apreciarse la clasificación:

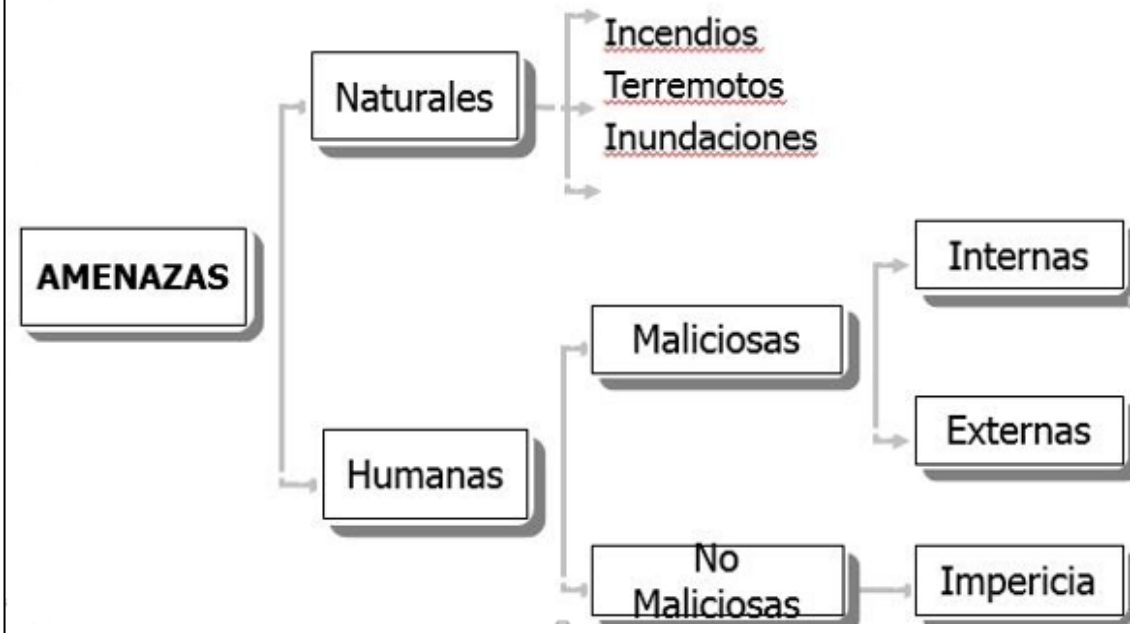


Figura 2. Clasificación de las amenazas informáticas.
Tomado de (ARCERT, Manual del Instructor de Seguridad, 2013)

1.2.2 Seguridad informática y Seguridad de la información

A pesar de que los términos se asemejan, Seguridad Informática y Seguridad de la Información tienen objetivos y actividades diferentes.

“La Seguridad Informática (IT Security) se describe como la distinción táctica y operacional de la Seguridad, mientras la Seguridad de la Información (Information Security) sería la línea estratégica de la Seguridad (Gonzalez, 2011)”.

Esto, en palabras más sencillas se refiere a que la Seguridad Informática tiene a su cargo las implementaciones técnicas para proteger la información, esto es firewalls, antivirus, DLP, correlacionadores, etc. Mientras que la Seguridad de Información se orienta al análisis de escenarios, buenas prácticas y aplicación de normativas para cumplir con la protección de la información.

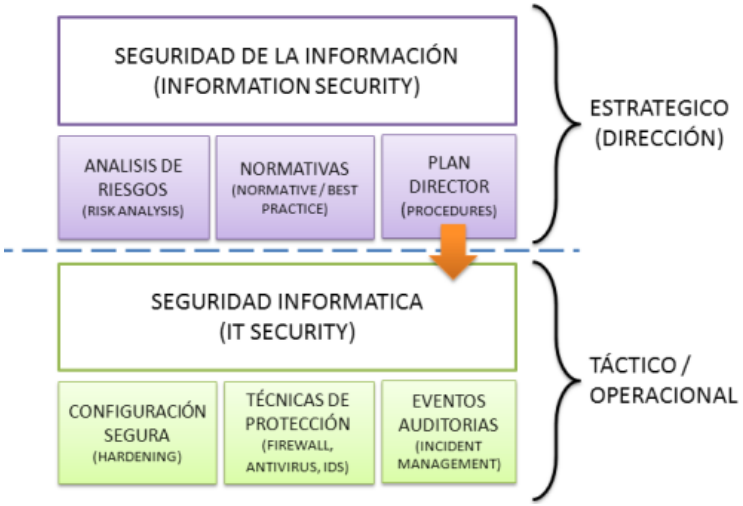


Figura 3. Seguridad de la Información vs Seguridad Informática

Tomado de http://www.seguridadparatodos.es

1.2.3 Requerimientos de seguridad de la información.

Para lograr un alcance efectivo de las prácticas de seguridad, la organización debe identificar claramente cuáles son sus requerimientos de seguridad. Para ello, se puede evaluar tres fuentes:

- La primera se enfoca en los objetivos y estrategias generales del negocio la cual permite realizar la valoración de los riesgos de la organización, las amenazas de los activos quedan identificadas, se calcula la vulnerabilidad y la probabilidad de ocurrencia y es factible evaluar el impacto en el negocio.
- Una segunda, es el conjunto de requerimientos legales, normativas, regulaciones y contratos que celebran la organización, sus accionistas, socios comerciales y los proveedores.
- Otra, está basada en los principios, objetivos y requerimientos del tratamiento de la información que la organización ha desarrollado para sus operaciones.

1.2.4 Impacto en la organización

Según (ARCERT, Manual de Seguridad en Redes, 2013), en cualquier implementación, sea tecnológica, administrativa o, como en este caso, normativa, el impacto a los usuarios en inevitable. Sin embargo, es factible tomar medidas que ayudarán a palear este impacto.

Por citar algunos, por ejemplo la disminución de la funcionalidad tal vez sea uno de los mayores problemas. Como cuando el usuario, para acceder a un sistema, debía realizar un solo login. Luego de la implementación del nuevo esquema de seguridad, debe realizar dos: uno para ingresar al sistema y otro para acceder al recurso. Por parte del usuario esto lo vive como un impedimento o traba en su tareas regulares, en lugar de verlo como una razón de seguridad para él mismo, pues así, se puede controlar más el uso del recurso y, ante algún problema, será mucho más fácil establecer responsabilidades.

Así mismo, al implementar esta nueva norma de seguridad, traerá una nueva tarea para la parte técnica y administrativa como cambiar los perfiles y accesos de algunos usuarios. Esto implica que se debe comunicarles por algún medio de los cambios realizados y en qué les afectará

1.3 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN (PSI)

“Una política proporciona a la gerencia la dirección y soporte para la gestión de seguridad de la información en concordancia con los requerimientos comerciales, las leyes y regulaciones relevantes(INEN, 2009)”.

Las PSI marcan el camino a seguir en la actuación del personal en relación con los recursos y servicios informáticos. Más que instrumentos sancionatorios, deben ser concebidos como expresiones de lo que se quiere proteger y por qué. Cada PSI debe apuntar a vigilar el uso y las limitaciones de los recursos y servicios informáticos críticos de la organización.

1.3.1 Elementos de una PSI

En materia de Seguridad de la Información hay múltiples criterios. Por ejemplo,(ARCERT, Manual de Seguridad en Redes, 2013), manifiesta que las PSI deberían considerar entre otros, los elementos a continuación:

- Alcance de las PSI, incluyendo facilidades, sistemas y personal sobre la cual aplica. Que debe interpretarse como una invitación de la empresa a cada miembro para que reconozca a la información como uno de sus principales activos, vital para el desarrollo del negocio. Es recomendable que esta invitación concluya en una posición.
- Objetivos y descripción concisa de los elementos involucrados.
- Responsabilidades por cada servicio y/o recurso informático a todos los niveles de la compañía.
- Requisitos mínimos para lograr la configuración de seguridad de los sistemas que involucra el alcance de la PSI.
- Establecimiento de violaciones y consecuencias del no cumplimiento de la PSI.
- Responsabilidades de los usuarios respecto a la información a la que tienen acceso.

Las PSI deben describir por qué deben tomarse ciertas decisiones, dar a entender y transmitir por qué son importantes los recursos o servicios en cuestión.

Así mismo, las PSI deben establecer las expectativas de la empresa en materia de seguridad. En lo posible, se debe manejar un lenguaje común, libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, procurando mantener su precisión y formalidad.

Las PSI deben especificar la autoridad responsable de que las cosas ocurran, los correctivos y las acciones que permitan dar indicaciones sobre las sanciones que se puedan imponer. No es recomendable especificar con exactitud qué pasara o cuándo algo sucederá. Recuérdese que no es una sentencia obligatoria de la ley.

“Finalmente, las PSI como documentos dinámicos de la organización, deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, cambio o diversificación de negocios entre otros(ARCERT, Manual de Seguridad en Redes, 2013)”.

1.3.2 Parámetros para establecer PSI

Las características de las PSI antes mencionadas, detallan la perspectiva en la formulación de las mismas. A continuación, se describen algunos aspectos generales recomendados para su formulación, según (ARCERT, Manual de Seguridad en Redes, 2013):

- Se recomienda efectuar un ejercicio de análisis de riesgos informáticos, el cual valore sus activos; esto le permitirá afinar las PSI de su organización.
- Las áreas propietarias de los recursos o servicios siempre deben ser tomadas en cuenta, pues son quien poseen la experiencia y son una fuente principal para establecer el alcance y las definiciones de violaciones a la PSI.
- Siempre es recomendable la comunicación a todo el personal involucrado en el desarrollo de las PSI. Es recomendable dar a conocer los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Es necesario identificar quién tiene la autoridad para tomar decisiones, pues son ellos los responsables de salvaguardar la integridad de la información de su área u organización.
- Una vez implementadas, desarrolle un proceso de monitoreo periódico de las políticas de la organización, que permita una actualización oportuna de las mismas.

Para tomar en cuenta: “no dé por hecho algo que es obvio. Haga explícito y concreto los alcances y propuestas de seguridad, con el propósito de evitar sorpresas y malos entendidos en el momento de establecer los mecanismos de seguridad que respondan a las PSI trazadas. (ARCERT, Manual de Seguridad en Redes, 2013)”

.

1.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

El dominio CONTROL DE ACCESO del estándar ISO 27002:2013 tiene como objetivo hacer limitado el acceso a la información y a las instalaciones de tratamiento de la misma. Consta de cuatro subdominios.

Este estudio se centra en el cuarto: Control de acceso a los sistemas y aplicaciones. Presenta los siguientes controles:

1.4.1 Restricción de acceso a la información

El objetivo de este control es basar la restricción de acceso a la información de acuerdo con la política establecida y los requerimientos del negocio.

“Debería considerarse lo siguiente para dar soporte a las funciones del sistema de aplicaciones:

a) Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación.
b) Controlar los datos que pueden ser accedidos por un usuario particular
c) Controlar los derechos de acceso de los usuarios; por ejemplo, lectura, escritura, eliminar y ejecutar.
d) Controlar los derechos de acceso de otras aplicaciones
e) Limitar la información contenida en las salidas.
f) Proporcionar controles de acceso físico o lógico para el aislamiento de las aplicaciones sensibles, datos de aplicación o sistemas. (Instituto Uruguayo de Normas Técnicas, 2014)”

1.4.2 Procedimientos seguros de inicio de sesión

Este control da pautas para un logueo seguro hacia los sistemas y aplicaciones, minimizando en lo posible el despliegue de información de los mismos. Propone también, el uso de métodos de autenticación.

“Un buen procedimiento de conexión (log-on) debería:

a) No mostrar identificación del sistema o aplicación hasta que termine el proceso de conexión.
b) Desplegar un mensaje genérico advirtiendo que el sistema debería accederse solamente por usuarios autorizados.
c) no ofrecer mensajes de ayuda al proceso de conexión que puedan guiar a los usuarios no autorizados.
d) Validar la información de conexión solo tras rellenar todos sus datos de entrada. Si se produce una condición de error, el sistema no debería indicar que parte de esos datos es correcta o incorrecta.
e) Proteger contra intentos de inicio de sesión por fuerza bruta
f) Registrar los intentos fallidos y exitosos.
g) Provocar un evento de seguridad si un potencial intento fallido o incumplimiento de los controles de acceso es detectado.
h) Mostrar la siguiente información acerca de la culminación de un inicio de sesión exitoso:
    1. Fecha y hora de la anterior conexión realizada con éxito.
    2. Detalles de cualquier intento de conexión fallido desde el momento de la última conexión realizada con éxito.
i) No mostrar la contraseña que está siendo ingresada.
j) No transmitir contraseñas por una red en texto limpio.

k) Terminar sesiones inactivas después de un periodo de inactividad definido, especialmente en las ubicaciones de alto riesgo, tales como en las áreas públicas o externas; fuera de la gestión de seguridad de la información o en los dispositivos móviles.
l) Restringir los tiempos de conexión para proporcionar seguridad adicional para aplicaciones de alto riesgo y reducir la ventana de oportunidades para el acceso no autorizado (Instituto Uruguayo de Normas Técnicas, 2014)"

Adicionalmente debe considerarse que las contraseñas son la forma más común de proporcionar identificación y autenticación basada en un secreto que solo el usuario conoce. Se puede trabajar para lograr lo mismo con medios criptográficos y protocolos de autenticación. La complejidad de la autenticación de un usuario debería ser proporcional a la importancia de la información a ser accedida.

1.4.3 Sistema de gestión de contraseñas

Este control propone directrices para gestionar las contraseñas asegurando la calidad de las mismas.

"Un sistema de gestión de contraseñas debería

a) Imponer el uso de contraseñas e identificaciones de usuario individuales con el fin de establecer responsabilidades.
b) Permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para evitar errores al introducirlas.
c) Imponer la selección de contraseñas de calidad

d) Forzar a los usuarios el cambio de contraseñas temporales en su primera conexión.
e) Hacer cumplir los cambios periódicos de contraseña, según sea necesario
f) Mantener un registro de las anteriores contraseñas utilizadas e impedir su reutilización.
g) No mostrar las contraseñas en la pantalla cuando se están introduciendo.
h) Almacenar archivos de contraseñas en lugares diferentes de los datos del sistema de aplicaciones.
i) Almacenar y transmitir contraseñas de forma protegida.(Instituto Uruguayo de Normas Técnicas, 2014)”

1.4.4 Uso de programas de utilidad privilegiados

En este control se proveen directrices para restringir y/o controlar el uso de programas utilitarios que pudieran anular los controles de aplicaciones y sistemas.

“Considerar:

a) El uso de procedimientos de identificación, autenticación y autorización para los programas de utilidad.
b) La separación de los programas de utilidad de las aplicaciones de software.
c) La limitación de uso de los programas de utilidad para un número mínimo de usuarios autorizados y de confianza.
d) La autorización para el uso especial de los programas de utilidad

e) La limitación de la disponibilidad de los programas de utilidad, por ejemplo, para la duración de un cambio autorizado.
f) EL registro de todo el uso de los programas de utilidad.
g) La definición y documentación de los niveles de autorización para los programas de utilidad.
h) La eliminación o desactivación de todos los programas de utilidad innecesarios.
i) No poner los programas de utilidad a disposición de los usuarios que tienen acceso a las aplicaciones donde la separación de funciones es requerida.(Instituto Uruguayo de Normas Técnicas, 2014)”

1.4.5 Control de acceso al código fuente de los programas

Este control va dirigido a restringir el acceso al código fuente de los programas. Menciona la importancia de controlar estrictamente su acceso para prevenir la manipulación desautorizada del código que pudiera introducir funcionalidades no permitidas, cambios involuntarios, etc.; además de que busca preservar la confidencialidad en temas de propiedad intelectual, así como también considera el almacenamiento centralizado del código en bibliotecas de programas fuente.

“Las directrices siguientes deberían ser consideradas para controlar el acceso a tales bibliotecas de programas fuente y para reducir la potencial corrupción de los programas computacionales:

a) De ser posible, las bibliotecas de programas fuente no deberían estar soportadas en sistemas de producción.
b) El código de los programas fuente y las bibliotecas fuente deberían gestionarse acorde a procedimientos establecidos.

c) El personal de soporte no debería tener acceso sin restricción a las bibliotecas de programas fuente.
d) La actualización de las bibliotecas de programas fuente y artículos asociados y la entrega de programas fuente a los programadores solo debería realizarse después de que la autorización apropiada ha sido recibida.
e) Los listados de programas deberían mantenerse en un ambiente seguro.
f) Debería mantenerse un registro de auditoría de todos los accesos a las bibliotecas de programas fuente.
g) El mantenimiento y la copia de bibliotecas de programas fuente deberían estar sujetos a estrictos procedimientos de control de cambios.

Si el código fuente del programa va a ser publicado, deberían considerarse controles adicionales para ayudar a conseguir garantías sobre su integridad.(Instituto Uruguayo de Normas Técnicas, 2014)”

CAPÍTULO II: ANÁLISIS DEL ESTADO ACTUAL Y LA FACTIBILIDAD DE LA IMPLEMENTACIÓN DE UNA NORMA INTERNACIONAL DE ACCESO

2.1 MARCO METODOLÓGICO

Dentro del marco metodológico, se puede afirmar que el tipo de estudio es descriptivo aplicado a una investigación mixta; ya que se elaborará un documento que se pondrá en práctica siguiendo los procesos definidos en la misma.

En cuanto al método usado, cabe mencionar al científico, deductivo e inductivo; ya que busca alinearse a un estándar internacional definido (ISO 27002:2013) para aplicarlo a la realidad de la Aseguradora del Sur iniciando con la recopilación de información mediante entrevistas y experiencias en base a las necesidades de la empresa; así como también la revisión de las mejores prácticas para realizar las políticas de seguridad del control de acceso.

En ese marco, se aplicará una investigación experimental porque no solo se va a identificar los riesgos en la Aseguradora del sur sino que se definirá políticas para reducirlos.

La recopilación de información acerca del estado actual del control de acceso a las aplicaciones se realizó a través de los siguientes métodos:

1. Entrevista personal con el Analista de Seguridad de la Información.
2. Análisis de arquitectura de aplicaciones en relación al control de acceso.
3. Informe de gestión del Analista de Seguridad de la información.

2.2 ANÁLISIS DE ACCESO ACTUAL A LAS APLICACIONES INFORMÁTICAS DE LA ASEGURADORA DEL SUR

2.2.1 Aplicaciones analizadas.

Para efectos del análisis, se ha tomado en cuenta las siguientes aplicaciones informáticas que forman parte de las actividades de la Aseguradora del Sur:

Visual Time.- El sistema Visual Time es el nuevo core de seguros de la compañía. Cuenta con menús, módulos y opciones específicas de acceso. Se coordinará con cada líder de proceso, los roles y esquemas definidos para cada uno de colaboradores que tengan acceso a la herramienta

PeopleSoft.- Sistema de Administración financiera - contable de la Aseguradora del Sur. Cuenta con menús, módulos y opciones específicas de acceso. Se coordinará con cada líder de proceso, los roles y esquemas definidos para cada uno de colaboradores que tengan acceso a la herramienta.

Digital Easy.- Es el sistema de Gestión Documental de Aseguradora del Sur. Cabe mencionar que el sistema no cuenta con controles de acceso, políticas y tampoco procedimientos que permitan garantizar la confidencialidad e integridad de la información ya que los usuarios que son creados se generan con contraseñas genéricas que no permiten el cambio al usuario final, además existen 1030 registros entre clientes, aps (Asesores Productores de Seguros) y usuarios internos que no se encuentran depurados, pudiendo encontrar ex-colaboradores de la compañía, brokers y clientes que ya no cuentan con relación comercial con Aseguradora del Sur, además se verifica que 146 usuarios cuentan con la opción “Gestión de Usuarios”, dicha opción permite al usuario poder administrar la herramienta al 100% y genera un riesgo de nivel

alto ya que al disponer de esta opción los usuarios pueden acceder a información confidencial, crear usuarios y modificar permisos de acceso.

Apex.- Es un sistema de reportes de información de Aseguradora del Sur. Dicha herramienta permite al usuario cambiar la contraseña únicamente en su primer inicio de sesión, es decir; si el usuario bloquea el aplicativo, el administrador definirá una clave única para el acceso, pudiendo esto generar riesgo ya que el usuario no contaría con una clave personal, además el sistema está compuesto por grupos de reportes al cual los colaboradores tienes acceso sin contar con una definición de perfiles de usuario, esto ocasiona que personal no autorizado pueda acceder a información confidencial.

SAF.- Administrado por el proceso Administrativo, el nuevo sistema de Activos Fijos, permite a los colaborares realizar la gestión de activos. Actualmente en implementación. Cuenta con menús, módulos y opciones específicas de acceso. Se coordinará con cada líder de proceso, los roles y esquemas definidos para cada uno de colaboradores que tengan acceso a la herramienta.

SAD.- De la misma forma el sistema de Archivo Digital es administrado por el proceso Administrativo, el cual permite digitalizar los documentos generados por la compañía y permitir la aprobación de facturas para el pago de los diferentes servicios que posee Aseguradora del Sur. El sistema cuenta con 11 servidores, uno por cada sucursal a nivel nacional, además cuenta con una clave única de administración a la que no es posible realizar el cambio de contraseña y de la misma forma al momento de crear un usuario se definirá una clave única, provocando riesgo en la confidencialidad e integridad de la información, la herramienta no se encuentra depurada por lo que se podrá

identificar registros de ex-colaboradores que ya no corresponden a la nómina de Aseguradora del Sur.

Evolution.- El sistema de Gestión del Talento. Actualmente en implementación en su nueva versión web. Cuenta con menús, módulos y opciones específicas de acceso. Se coordinará con cada líder de proceso, los roles y esquemas definidos para cada uno de colaboradores que tengan acceso a la herramienta.

2.2.2 Análisis FODA

Tabla 1

Fortalezas:	Debilidades:
1. Conocimiento técnico de la infraestructura tecnológica 2. Buena relación con el área de Riesgos 3. El departamento de seguridad de la información, está interesado en implementar estándares internacionales	1. Insuficiente poder de decisión sobre la infraestructura. 2. Falta de experiencia en implementación de normas internacionales de seguridad de la información. 3. No se administra todas las aplicaciones críticas del negocio.
Oportunidades:	Amenazas:
1. La infraestructura podría adaptarse a las necesidades del proyecto 2. Oportunidad de avanzar en el proyecto conjuntamente con el proceso de Riesgos.	1. Negativa de las autoridades al cambio. 2. Falta de tiempo para culminar 3. Renuencia de los usuarios a los cambios que implica implementar las

3. El proyecto crea una oportunidad que aporta competitividad a la organización.	políticas

2.2.3 Reseña histórica de la empresa

Aseguradora del Sur nació el 11 de febrero de 1990 en Cuenca con el objetivo de brindar a los ecuatorianos la mayor protección, en todo momento y lugar, siempre con un respaldo incondicional y bajo los conceptos de fortaleza y solidez.

En 1994 trasladamos nuestra matriz a Quito y a partir de 1997 Aseguradora del Sur decidió expandirse en la geografía ecuatoriana abriendo sucursales en: Ambato, Cuenca, Ibarra, Loja, Machala, Manta, Portoviejo, Riobamba, Santo Domingo, Francisco de Orellana (El Coca) y en el sur de Quito. Cada una de nuestras plazas tiene autonomía suficiente para comercializar seguros, brindando un mejor y más amplio servicio y experiencia a todos nuestros clientes.

La Aseguradora del Sur es una empresa de seguros con 25 años de presencia en el mercado ecuatoriano. Se trata de una empresa con alrededor de 300 empleados de los cuales al menos 250 son usuarios de un computador. El giro del negocio de seguros exige manejar y gestionar una gran cantidad de información inherente a la actividad como clientes, proveedores, brokers, inspectores, talleres, etc. Por ello, el uso de aplicaciones informáticas es indispensable para el trabajo diario. Por lo expuesto, la aseguradora cuenta con varias herramientas y/o sistemas informáticos para acceder, consultar,

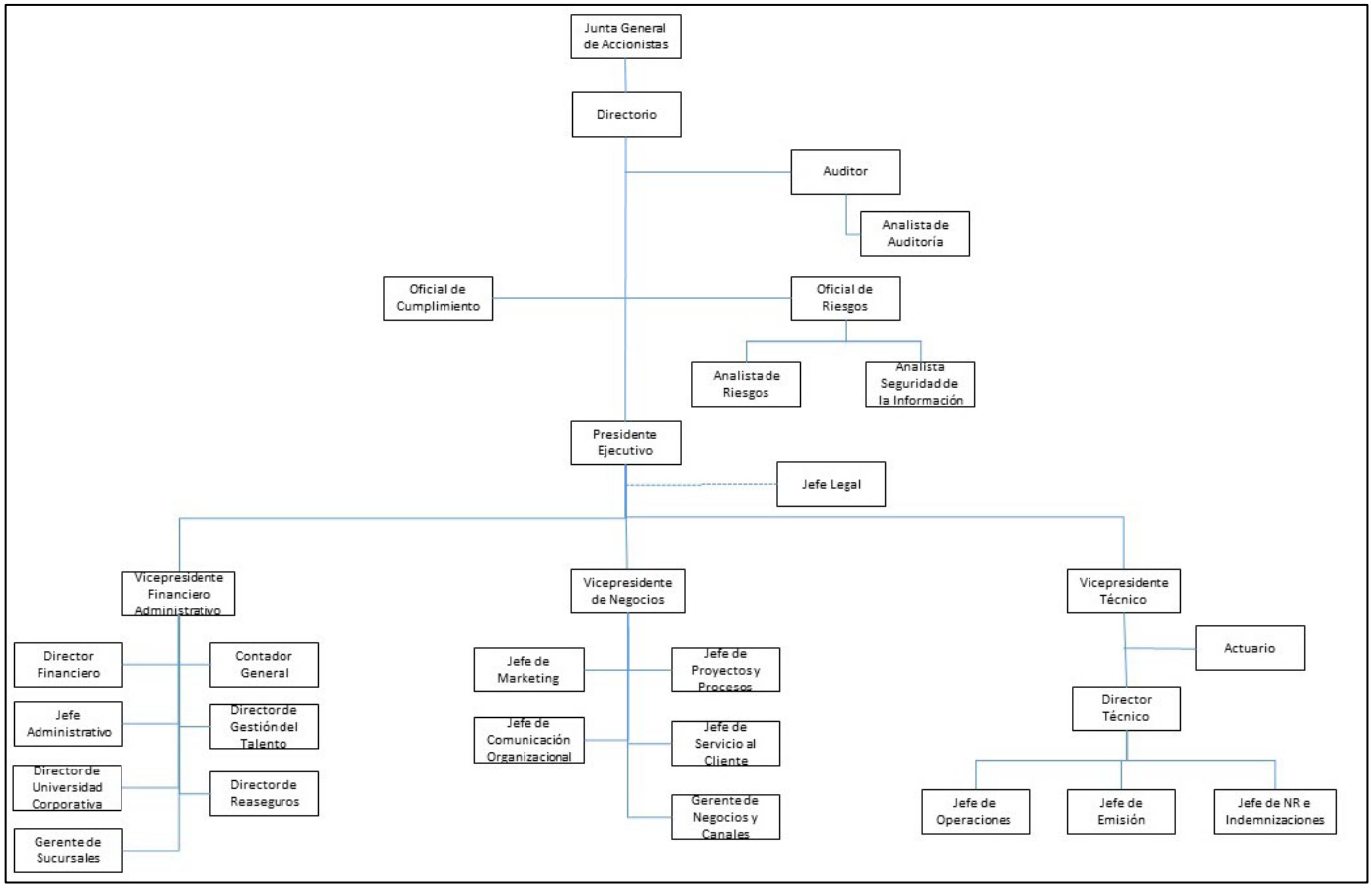
actualizar y verificar información de cada uno de los procesos de producción de pólizas de seguros

SITIO WEB:

www.aseguradoradelsur.com.ec

Figura 4. Logo de Aseguradora del Sur
Tomado de www.aseguradoradelsur.com.ec

2.2.4 Organigrama de la empresa



Como se puede apreciar, el Analista de Seguridad de la Información se encuentra subordinado al Oficial de Riesgos. Desde ahí, apoya directamente las decisiones que se toman a nivel de Directorio.

2.2.4.1 Objetivo del Analista de Seguridad de la Información:

Concentrar a través del proceso de Seguridad de la Información, la administración de todos los aplicativos de Aseguradora del Sur, estableciendo políticas y procedimientos que garanticen la disponibilidad, integridad, confidencialidad, control de accesos y legalidad de la información.

2.3 ANÁLISIS DE FACTIBILIDAD DE IMPLEMENTACIÓN DE LAS MEJORES PRÁCTICAS DE CONTROL DE ACCESO.

2.3.1 Análisis de la información

Para el desarrollo del tema de tesis se realizó un análisis de las aplicaciones factibles a implementarla tomado en cuenta las fuentes citadas en la sección Marco Metodológico. Estas son:

1. Entrevista personal con el Analista de Seguridad de la Información.
2. Análisis de arquitectura de aplicaciones en relación al control de acceso.
3. Informe de gestión del Analista de Seguridad de la información.

Las mismas pueden observarse en la sección Anexos.

De aquello, podemos concluir lo siguiente:

1. Existe un proyecto de establecimiento de Políticas de Seguridad de la información que está parcialmente fundamentado en estándares internacionales. El proyecto está suspendido y, en su mayor parte, se ha implementado empíricamente.

2. El mencionado proyecto, al no basarse en ISO 27002, no habla explícitamente de la sección “Control de acceso a las aplicaciones”.
3. Las aplicaciones de la Aseguradora del Sur presentan una variedad de arquitecturas, propias del tiempo en que se desarrollaron. Por ello, no todas son factibles a aplicar el Control de acceso.
4. No existe un inventario actualizado de los roles y perfiles de acceso para los usuarios.
5. El control de acceso a las aplicaciones está parcialmente controlado por el Analista de Seguridad de la información.
6. Debido a la arquitectura desplegada en las aplicaciones críticas de la Aseguradora del Sur, no podemos establecer un “sistema confidencial” tal como se presenta en el estándar ISO/IEC 27002:2013; ya que cada sistema se relaciona con otros para enviar y consumir datos importantes a varios niveles.

Por todo esto, se hace necesario el desarrollo del presente proyecto que propondrá el establecimiento de un estándar internacional (ISO/IEC 27002:2013) para el “Control de acceso a las aplicaciones” informáticas de la Aseguradora del Sur.

2.3.2 Aplicaciones informáticas de la aseguradora del sur factibles a implementar el estándar ISO/IEC 27002:2013

Una vez realizado el análisis de las aplicaciones informáticas de la Aseguradora del Sur, se determina como factibles a implementar la sección “Control de acceso a las aplicaciones” según el estándar ISO 27002:2013 a las siguientes aplicaciones:

1. Visual Time

2. PeopleSoft
3. SAF
4. Evolution

CAPÍTULO III: IMPLEMENTACIÓN DEL ESTÁNDAR ISO/IEC 27002:2013 SECCIÓN "CONTROL DE ACCESO A LOS SISTEMAS Y APLICACIONES"

3.1 MANUAL DE SEGURIDAD DE LA INFORMACIÓN, SECCIÓN CONTROL DE ACCESO A LOS SISTEMAS Y APLICACIONES.

El presente manual contiene la política de seguridad de la información que define el accionar del personal, sus responsabilidades y la revisión y/o actualización de la misma.

De igual manera, contiene políticas y procedimientos que guiarán al personal de seguridad de la información para el establecimiento de accesos hacia las aplicaciones y sistemas en la Aseguradora del Sur basado en el estándar ISO/IEC 27002:2013; es decir, se puede encontrar los procedimientos adecuados para establecer un acceso seguro orientado a cumplir los estándares de seguridad internacionales garantizando la confidencialidad, integridad y disponibilidad de la información.

3.2 PROPUESTA DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Las disposiciones establecidas en este documento deben incorporarse como parte de las actividades normales de los colaboradores y aplicarse también en las relaciones con terceros.

En una cultura preventiva, ante cualquier duda lo primero es preguntar a los niveles apropiados, decidir por cuenta propia o a la ligera expone a la compañía a consecuencias desfavorables.

1. Aseguradora del Sur implementará las políticas, procesos y procedimientos, aprobados por el Directorio, para garantizar la

confidencialidad, integridad y disponibilidad de la información, aquella que es de su propiedad y la que se encuentre bajo su responsabilidad, considerando mecanismos de protección adecuados en medios físicos y electrónicos, y la conocida por los colaboradores y proveedores en las relaciones con Aseguradora del Sur

2. Las políticas de seguridad de la información podrán ser actualizadas en los siguientes casos:

• En cualquier momento cuando existan propuestas debidamente sustentadas por parte de la alta gerencia.

• Por cambios significativos en la tecnología de la información que requiera ajustes importantes de seguridad y que sean propuestos por el analista de seguridad de la información

• Revisión anual de este documento por parte del analista de seguridad de la información.

3. Estas políticas, procesos y procedimientos serán publicadas en la intranet para conocimiento de todos los colaboradores, a partir de la cual su cumplimiento será obligatorio, incluso el personal nuevo estará en la obligación de conocerlas previo a iniciar sus actividades.

4. El contenido de estas políticas se aplicarán incluso a las relaciones con proveedores que manejen información sensitiva, riesgosa o sus actividades sean críticas para Aseguradora del Sur.

5. Es responsabilidad del proceso de Riesgos, el realizar un plan de capacitación, educación y formación a todos los colaboradores de Aseguradora del Sur, que deban cumplir con las regulaciones, normas y procedimientos de esta política.

3.3 PROPUESTA DE PROCEDIMIENTOS PARA CONTROL DE ACCESO A LAS APLICACIONES

3.3.1 Restricción de acceso a la información

CONTROL:

"El acceso a la información y a las funciones del sistema de aplicaciones debería restringirse de acuerdo con la política de control de acceso. (Instituto Uruguayo de Normas Técnicas, 2014)"

3.3.1.1 Procedimientos:

1. Todas las aplicaciones de Aseguradora del Sur autenticarán la identidad de los usuarios antes de ingresar a su funcionalidad.

2. Aseguradora del Sur permitirá el acceso a las aplicaciones informáticas únicamente a usuarios autorizados por el negocio.

3. La creación de un nuevo usuario y accesos a los sistemas de información de Aseguradora del Sur, serán solicitados por medio de correo electrónico al Analista de seguridad; quien aprobará los accesos, en base a una matriz de perfiles por cargo. La asignación de

credenciales para autenticación en las distintas aplicaciones será secreta y controlada a través de un documento impreso que deberá ser firmado por el Analista de Seguridad de la Información y el usuario receptor.

4. Los controles de acceso serán documentados, revisados y actualizados anualmente, sobre la base de requerimientos aprobados por el negocio.

5. Los usuarios serán registrados y sus accesos asignados, modificados o eliminados, mediante un proceso regular y documentado.

6. Los usuarios tendrán una identificación única por plataforma tecnológica, mientras no se disponga de un mecanismo que permita tener una identificación para varias o todas las plataformas.

7. La entrega de claves de acceso a los diferentes sistemas de información, serán temporales y el usuario tendrá la obligación de cambiarlas en su primer inicio de sesión, además deberá tomar en cuenta que la clave de acceso es personal y totalmente intransferible para todos los sistemas.

8. Los usuarios serán responsables por toda la actividad ligada con su identificación, por lo tanto no la deben dar a conocer ni compartirla con otras personas. Los usuarios están prohibidos de dar a conocer sus contraseñas a personal no autorizado, en caso de suscitarse este

particular, se tomarán las acciones administrativas o contractuales que correspondan. En caso de proveedores, se procederá al cambio inmediato de las mismas.

9. En el caso de que la administración de cualquier acceso a aplicaciones esté a cargo de un tercero o proveedor, este deberá canalizarla a través de la unidad de riesgos para que este a su vez sea quien registre los accesos a dichos sistemas, como también deberá cumplir con todos los requisitos establecidos en las políticas y procedimientos de Aseguradora del Sur , el incumplimiento de los mismos, aun cuando no se tenga evidencia de haberse materializado, acarreará la sanción pecuniaria establecida en el contrato y la terminación unilateral del mismo.

10. Todo sistema o aplicación que contenga información referente al negocio como pólizas, tasas, valores, contratos, clientes, proveedores, reaseguros y relacionados deberá ser tratado como confidencial. De igual manera la información referente a la administración del negocio tal como ingresos, balances, y cualquier dato de carácter financiero – contable.

11. Todos los perfiles de acceso de usuarios serán retirados o modificados ante la terminación de la relación laboral, contractual o comercial, y ante cambio de funciones. Los coordinadores serán los responsables de solicitar la eliminación de tales perfiles al Analista de seguridad de

información dentro de un periodo de 24 horas, mediante la comunicación por correo.

12. Los dueños de los procesos revisarán los perfiles o roles de acceso de usuarios una vez al año o bajo demanda

13. Aseguradora del Sur limitará a los usuarios el acceso a la información estrictamente necesaria para cubrir sus necesidades funcionales, a través de acceso por usuario y perfiles respectivos.

14. En el caso de integraciones con otros sistemas, los dueños de los procesos serán los encargados de autorizar y dar a conocer, vía email, al Analista de Seguridad de la Información los procedimientos y/u objetos que intervienen en la integración.

15. El Analista de la Información deberá comunicar, vía email, los riesgos a los que se expone la información al integrar los sistemas.

16. El dueño del proceso asumirá los riesgos comunicados por el Analista de Seguridad y esto deberá quedar firmado en un documento.

3.3.1.2 Procedimientos de creación y depuración de usuarios y perfiles

Siempre y cuando la arquitectura de la aplicación lo permita, los username deberían establecerse de la siguiente forma:

a. Se toma la inicial del primer nombre y el apellido completo usando solo caracteres sin tilde, diéresis u otra letra que incluya un símbolo especial como la “ñ”.
b. Si hay dos usuarios que generan el mismo username, se eliminará el conflicto generando el username normal para aquel que, considerando su segundo nombre, esté alfabéticamente primero; y para el segundo, se usará la inicial del primer nombre, la inicial del segundo nombre y el apellido completo.
c. Si hay un usuario nuevo que entra en conflicto con un existente, se aplica el criterio anterior (b) para el nuevo usuario.
d. Si hay más de 2 usuarios que generan conflicto, se usa la primera letra del segundo apellido para eliminar el conflicto.
e. Si existiera el caso de un usuario donde la aplicación de la regla implica la generación de un username que resulta inadecuado, se aplica el criterio (b) previa consulta con el usuario afectado.
f. Todas las letras del username deben ser minúsculas
g. No se puede generar un username que, por su forma sugiera que el usuario tiene cierta autoridad en los sistemas o accesos. Nombres como admin, super, supervisor, gerente, Administrador, root, sa y similares están prohibidos para los usuarios finales.

3.3.2 Procedimientos seguros de inicio de sesión.

CONTROL

“El acceso a los sistemas y aplicaciones debería controlarse mediante procedimientos de conexión (log on) seguros, cuando lo requiera la política de control de acceso. (Instituto Uruguayo de Normas Técnicas, 2014)”

PROCEDIMIENTOS:

1. Todos los accesos a los sistemas de información, cuando su tecnología lo permita, exhibirán un aviso informativo acerca del buen uso y propiedad de la información en pantalla que señale la obligatoriedad del usuario de utilizar los recursos de Aseguradora del Sur para propósitos de negocio; que toda la información almacenada, transmitida o visualizada es de propiedad de Aseguradora del Sur y el uso de la información será revisada y supervisada con fines administrativos y legales.
2. Las ventanas de acceso a las aplicaciones no deberán desplegar títulos, descripciones o textos que describan la información a la que se va a acceder antes de loguearse.
3. Todas las aplicaciones deberán tener habilitados logs para almacenar toda la actividad de inicio de sesión.
4. Las aplicaciones deberán tener un tiempo de caducidad de sesión determinado por cada dueño de proceso.
5. Ninguna aplicación estará habilitada para el acceso externo a la LAN, salvo estudio y autorización del Analista de Seguridad.

3.3.3 Sistema de gestión de contraseñas:

CONTROL

“Los sistemas de gestión de contraseñas deberían ser interactivos y debería asegurar la calidad de las contraseñas. (Instituto Uruguayo de Normas Técnicas, 2014)”

PROCEDIMIENTOS:

Aseguradora del Sur implementará un proceso interactivo de gestión de contraseñas y garantizará contraseñas adecuadamente estructuradas, así:

1. Las contraseñas nunca deben aparecer e ingresarse en pantalla en texto claro, ni almacenarlas de igual manera, además las contraseñas se deben mantener confidenciales en todo momento.

2. Las contraseñas estáticas deben cumplir con las siguientes condiciones:

- Estructurarse con un mínimo de 6 caracteres, los cuales deben tener combinaciones de letras y números.
- Obligarse el cambio de la contraseña inmediatamente luego de la creación del usuario o de reinicio de contraseña.
- Cambiarse obligatoriamente cada tres meses para usuarios internos, y para usuarios externos e internos brindar la opción para que la puedan cambiar en cualquier momento, señalando la importancia de cambiar la contraseña frecuentemente.
- Las contraseñas mal ingresadas en 3 intentos consecutivos serán bloqueadas, y habrá un proceso documentado para reactivarla.
- Las identificaciones no utilizadas por un año serán eliminadas.

3.3.4 Uso de programas de utilidad privilegiados

CONTROL:

“El uso de programas de utilidad que podrían ser capaces de anular el sistema y los controles de aplicación debería se restringido y estrictamente controlado. (Instituto Uruguayo de Normas Técnicas, 2014)”

PROCEDIMIENTOS:

1. Aseguradora del Sur no permitirá el uso de programas utilitarios que sean capaces de vulnerar los controles de sistemas y aplicaciones,
2. En casos excepcionales, como pruebas de concepto, demos o similares, aprobado por la unidad de riesgos, serán utilizados por un periodo limitado, justificadamente y estrechamente controlado por personal de la unidad de riesgos y de auditoría interna.

3.3.5 Control de acceso al código fuente de los programas

CONTROL

“El acceso al código fuente de los programas debería ser restringido. (Instituto Uruguayo de Normas Técnicas, 2014)”

PROCEDIMIENTOS:

1. En el caso de llegar a contar con código fuente de cualquier programa; éste será almacenado en un equipo exclusivo.
2. El acceso al código fuente será restringido para los usuarios.
3. En caso de requerirlo, el Analista de Seguridad autorizará el acceso al código previa firma de un documento de responsabilidad.

IV. CONCLUSIONES

1. Según el estándar ISO/IEC 27002:2013, el acceso a las aplicaciones de la Aseguradora del Sur presenta riesgos a la integridad a la información.

2. Actualmente, en la Aseguradora del Sur no existe un control de acceso regulado por ningún estándar internacional.

3. En la mayoría de controles de acceso a las aplicaciones se han aplicado controles de forma empírica.

4. Las aplicaciones de la Aseguradora del Sur presentan varias arquitecturas, propias de los desarrolladores y la época en que se construyeron. Por ello, no todas son factibles a aplicar el Control de acceso, tal como define el estándar ISO/IEC 27002:2013.

5. Actualmente, el control de acceso a las aplicaciones está parcialmente controlado por el Analista de Seguridad de la información

6. Actualmente, en la Aseguradora del Sur no existen ambientes dedicados para los “sistemas confidenciales”. Por lo tanto se incumple lo establecido en el estándar ISO/IEC 27002:2013

7. El cumplimiento de las políticas y procedimientos desarrollados coadyuvará a minimizar los riesgos asociados a los activos de la información. Esto se reflejará en reducción de impactos, control de fuga de información y disminución de pérdidas económicas.

V. RECOMENDACIONES

1. Este proyecto debería implementarse en el menor plazo posible; y debería ser coordinando con los procesos de Comunicación, Marketing que apoyan en la difusión del mismo.
2. Esta implementación debería constituirse en el punto de partida para el establecimiento de políticas que incluyan el cumplimiento de estándares internacionales.
3. Se debería organizar la actualización y/o modificación de las aplicaciones que no tienen capacidad de crear roles y perfiles de usuario.
4. La administración de usuarios debería estar centrada hacia el proceso de Riesgos en su totalidad.
5. Debido a la necesidad de optimizar Seguridad de la Información y la cantidad de usuarios y aplicaciones, debería constituirse un equipo de Seguridad de la Información que apoye al establecimiento de políticas y procesos estandarizados de seguridad.

GLOSARIO DE TÉRMINOS

APS: Agente Asesor Productor de Seguros

Cliente: Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una estación de trabajo que solicita el contenido de un archivo a un servidor es un cliente de este servidor. Ver también: "client-server model", "server".

Criptografía: La rama del conocimiento que se encarga de la escritura secreta, originada en el deseo humano por mantener confidenciales ciertos temas.

Dominio: Conjunto de computadoras que comparten una característica común, como el estar en el mismo país, en la misma organización o en el mismo departamento. Cada dominio es administrado por un servidor de dominios.

Firewall: "Es un sistema diseñado para evitar accesos no autorizados desde o hacia una red privada. Los Firewalls pueden estar implementados en hardware o software, o una combinación de ambos. Los firewalls son frecuentemente utilizados para evitar el acceso no autorizado de usuarios de internet a redes privadas conectadas a la misma, especialmente intranets. Todos los mensajes que dejan o entran a la red pasan a través del firewall, el cual examina cada mensaje y bloquea aquellos que no cumplan con determinado criterio de seguridad. (Sepúlveda, 2016)"

Host (sistema central): Computador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet y FTP.

Información. Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Intranet. Una red privada dentro de una compañía u organización que utiliza el mismo software que se encuentra en Internet, pero que es solo para uso interno.

ISO: Sigla de la expresión inglesa International Organization for Standardization, 'Organización Internacional de Estandarización', sistema de normalización internacional para productos de áreas diversas.

Log: Registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le va añadiendo líneas a medida que se realizan acciones sobre el sistema. Se utiliza en muchos casos distintos, para guardar información sobre la actividad de sistemas variados.

Login: En el ámbito de seguridad informática, login o logon es el proceso mediante el cual se controla el acceso individual a un sistema informático mediante la identificación del usuario utilizando credenciales provistas por el usuario

Navegador: Aplicado normalmente a programas usados para conectarse al servicio de exploración web.

Protocolo Descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes.

PSI: Políticas de Seguridad de la Información.

Seguridad: es “calidad de seguro”, y, seguro está definido como “libre de riesgo”.

SGSI: Sistema de Gestión de Seguridad de la Información

Username: Nombre del usuario, nombre único con el que un usuario es identificado al acceder a un sistema de multiusuarios (Informática)

Usuario: Sujeto o proceso autorizado para acceder a datos o recursos.

REFERENCIAS

ARCERT. (1 de 1 de 2013). *Manual de Seguridad en Redes.* Obtenido de http://instituciones.sld.cu/dnspminsap/files/2013/10/Manual-de-Seguridad-de-Redes.pdf

ARCERT. (2013). *Manual del Instructor de Seguridad.* Obtenido de http://econ.unicen.edu.ar/monitorit/index.php?option=com_docman&task=doc_download&gid=213&Itemid=19

Arteitio, J. (2008). *Seguridad de la Información.* Madrid: Paraninfo.

Gonzalez, J. (6 de 10 de 2011). *Seguridad para todos.* Obtenido de www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

Gutierrez, C. (12 de Diciembre de 2013). *welivesecurity.com.* Obtenido de http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/

INEN. (2009). *Norma Ecuatoriana ISO/IEC 27002.* Quito: INEN.

Instituto Uruguayo de Normas Técnicas. (2014). *UNIT-ISO-IEC 27002-2013_(ES).* Obtenido de https://es.scribd.com/document/264424191/UNIT-ISO-IEC-27002-2013-ES

Sepúlveda, D. F. (2016). *Glosario de Términos en Redes y Seguridad.* Obtenido de http://diegoforever.wikispaces.com/file/view/Glosario-de-Terminos-en-Redes-y-Seguridad.pdf

ANEXOS