ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría En Seguridad Informática Aplicada

“ANÁLISIS E IMPLEMENTACIÓN DEL MANUAL DE POLÍTICAS Y NORMAS DE CONTROL DE ACCESO PARA LA EMPRESA IMPVET IMPORTADORA VETERINARIA CÍA. LTDA.”

EXAMEN DE GRADO (COMPLEXIVO)

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

PAOLO FRANCISCO MARTÍNEZ ZEA

GUAYAQUIL – ECUADOR

AÑO: 2016

AGRADECIMIENTO

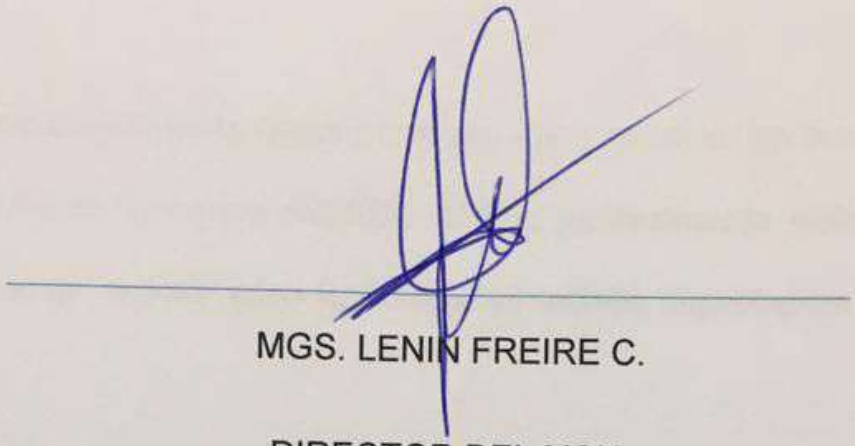
Primero agradezco a Dios, mi Señor, que me permitió cursar y terminar esta meta personal tan anhelada. A mi familia, siempre siendo el soporte de mi vida. A mi esposa, gracias especiales por la paciencia. A Matteo, por estar conmigo pasando tantas malas noches.

A Impvet Importadora Veterinaria Cía. Ltda. y a la ESPOL por ayudarme en la culminación de este proyecto.

DEDICATORIA

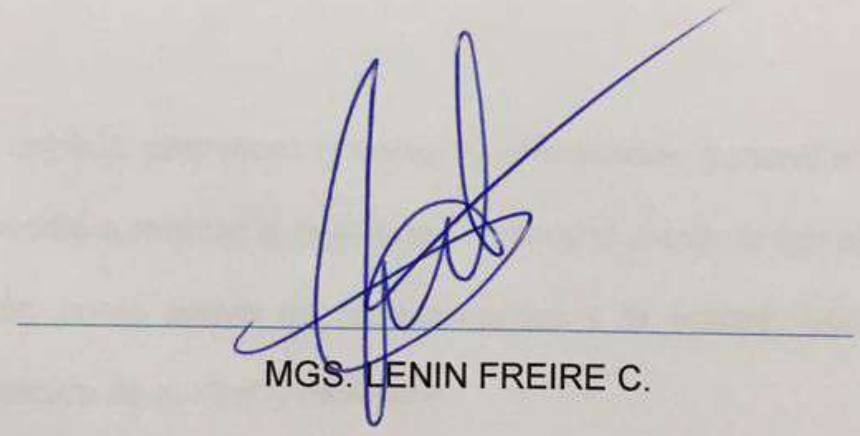
El presente proyecto de investigación se lo dedico a mi esposa, todo lo que soy y lo que hago es por ti, mi princesa.

TRIBUNAL DE SUSTENTACIÓN



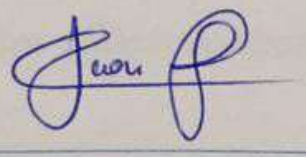
MGS. LENIN FREIRE C.

DIRECTOR DEL MSIA



MGS. LENIN FREIRE C.

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA



MGS. JUAN CARLOS GARCÍA

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

RESUMEN

El presente documento tiene como propósito dar a conocer las buenas prácticas de seguridad mediante la norma ISO/IEC 27000, puntualmente enfocada al dominio A11 de control de acceso para la compañía Impvet Importadora Veterinaria Cía. Ltda.

En el primer capítulo podremos observar la información general sobre la compañía donde se procedió a realizar la investigación para el presente trabajo, la importancia de información como activo de toda empresa y la norma ISO/IEC 27000, sus dominios, objetivos de control y controles.

En el segundo capítulo se establece el marco metodológico, tipo de investigación, método de investigación y las fuentes y técnicas para la recolección de información.

En el tercer capítulo, basados en la infraestructura y situación actual de la compañía en estudio, analizamos uno a uno los controles mediante listados de chequeo y presentamos los resultados y observaciones de la investigación.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad la tecnología avanza a pasos agigantados, el aumento de la interconectividad y la globalización causada por el internet y su auge nos permite prepararnos de mejor manera para hacerle frente a todo tipo de situaciones corporativas, tanto internas como externas.

Es frecuente escuchar en las noticias sobre delitos informáticos o ataques a la información corporativa y es esta una de esas oportunidades para prepararnos de la mejor manera posible y mantener la disponibilidad, integridad y confidencialidad de nuestra información, aplicando buenas prácticas mundiales de seguridad que se encuentran condensadas en check-list, procesos y controles. Una de las preocupaciones más importantes en la actualidad para las compañías es la seguridad de su información

El control de acceso es sin duda parte fundamental de la infraestructura de seguridad de un sistema. En el mundo real al acceder a una bóveda de un banco es notorio el número de medidas de control que tiene para proteger su contenido, en una compañía su activo más preciado es la información y esta debe ser tratada de la misma manera que si se encontrara en esa bóveda del banco.

CAPÍTULO 1

1. GENERALIDADES

1.1. Antecedentes

Impvet Importadora Veterinaria Cía. Ltda. empieza sus operaciones comerciales en Ecuador con la distribución exclusiva de las líneas de productos veterinarios de MSD Salud Animal (antes Intervet International) e inmediatamente se convierte en uno de los líderes del mercado veterinario del país.

Con su matriz en la ciudad puerto Guayaquil cubre las necesidades del mercado avícola, porcino y ganadero con una amplia gama de productos, con representantes de ventas para la Costa, Sierra y Oriente respectivamente, así como también con Médicos Veterinarios especializados que contribuyen con el soporte técnico a las necesidades de cada sector.

El 2016, su departamento de TI trabajará en el proyecto de implementación de buenas prácticas para la gestión de la seguridad de la información con la finalidad de la protección de sus activos. El presente trabajo de investigación tiene por alcance uno de los dominios que se desea asegurar.

1.2. Descripción del problema

La empresa Impvet Importadora Veterinaria Cía. Ltda., es una empresa relativamente nueva y en crecimiento que posee usuarios, equipos de computación y aplicaciones que se integran entre ellos. Es indispensable contar con políticas, normas de seguridad de la información y buenas prácticas que permitan fluir de mejor manera la información entre las aplicaciones y procesos de la compañía.

En la actualidad existen pocas políticas de seguridad y controles, lo que evidencia un fuerte problema de seguridad en la infraestructura de la empresa, esto ha motivado a la Gerencia a la imperiosa necesidad de elaborar e implementar un manual de políticas y normas de seguridad en el control de acceso.

1.3. Solución Propuesta

Para poder cubrir la necesidad de Gerencia y brindar las seguridades necesarias al acceso de los activos de Impvet Importadora Veterinaria Cía.

Ltda., procederemos a realizar un análisis considerando el estándar de seguridad ISO/IEC 27000 y la elaboración del manual de políticas y normas de control de acceso considerando los temas de usuarios y sus responsabilidades, de las redes y de los sistemas y aplicaciones.

1.4. Objetivo General

Analizar e implementar un manual de políticas y normas para controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática para Impvet Importadora Veterinaria Cía. Ltda.

1.5. Marco Teórico

1.5.1. Información

Según la CNSS (2010) al hablar de información nos referimos a cualquier comunicación o representación del conocimiento como hechos, datos u opiniones en cualquier medio o forma, incluso textual, numérico, gráfico, cartográfica, la narrativa, o audiovisual. [1]

Dicha información tiene valor para la organización, es considerado por ende un preciado activo de la misma. En la actualidad y con el gran crecimiento de las nuevas tecnologías de la comunicación y la

información las vulnerabilidades y amenazas son mayores y se debe estar preparado.

Maya y Jaramillo (2015) nos indican algo similar “ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio”. [2].

Figura 1.1 Amenazas para la seguridad

Es necesario conocer estas amenazas y vulnerabilidades, para con un correcto análisis poder implementar controles, procesos y buenas prácticas a fin de procurar la integridad, confidencialidad y disponibilidad de la información de nuestra organización.

1.5.2. Aseguramiento de la Información

El CNSS define al aseguramiento de la información como las "medidas que defiendan y protejan la información garantizando sus principios (disponibilidad, integridad, autenticación, confidencialidad y no repudio). Estas medidas incluyen la prestación para la restauración de los sistemas de información mediante la incorporación de capacidades de protección, detección y reacción". [1]

Es decir, la seguridad de la información se refiere a los controles, políticas, procedimientos y buenas prácticas que me permitirán proteger mi información de las amenazas y vulnerabilidades y poder así asegurar la continuidad de mis operaciones.

1.5.3. Principios básicos de la seguridad de la información

El Comité de Seguridad de la Información de la Universidad Tecnológica Nacional de Argentina (2009), es su plan de Políticas de Seguridad de la Información define lo siguiente:

- **Integridad:** Verificar la exactitud y totalidad de la información y de los métodos de procesamiento ingresados por personas o sistemas con acceso autorizado. [3]

- **Confidencialidad:** Verificar que la información sólo es accesible por personas o sistemas autorizados a tener acceso.[3]
- **Disponibilidad:** Verificar que las personas o sistemas autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. [3]

Figura 1.2 Principios básicos de la seguridad de la información

1.5.4. Políticas de Seguridad

"Agregado de directivas, reglamentos, normas y prácticas que prescriben cómo una organización gestiona, protege y distribuye la información". [1]

En otras palabras, una política de seguridad es el conjunto de reglas y procedimientos que informan que está permitido y que no dentro de la organización.

1.5.5. ISO/IEC 27000

La norma ISO/IEC 27000 hace referencia a los estándares de seguridad publicados por la ISO (Organización Internacional para la Estandarización) y la IEC (Comisión Electrónica Internacional), esta norma está organizado en base a los 11 dominios, 39 objetivos de control y 133 controles. [4]

Usaremos la siguiente tabla para enumerar los 11 dominios que posee la norma ISO/IEC 27000:2005, sus objetivos de control y sus controles.

Tabla 1. Dominios de ISO/IEC 27000:2005 [4]

Dominio	Objetivos de control	Controles
Política de seguridad	1	2
Organizando la seguridad de información	2	11
Gestión de activos	2	5
Seguridad ligada a recursos humanos	3	9
Seguridad física y ambiental	2	13
Gestión de comunicaciones y operaciones	10	32
Control de acceso	7	25
Adquisición, desarrollo y mantenimiento de sistemas de información	6	16
Gestión de incidentes de los sistemas de	2	5

información		
Gestión de la continuidad del negocio	1	5
Cumplimento	3	10

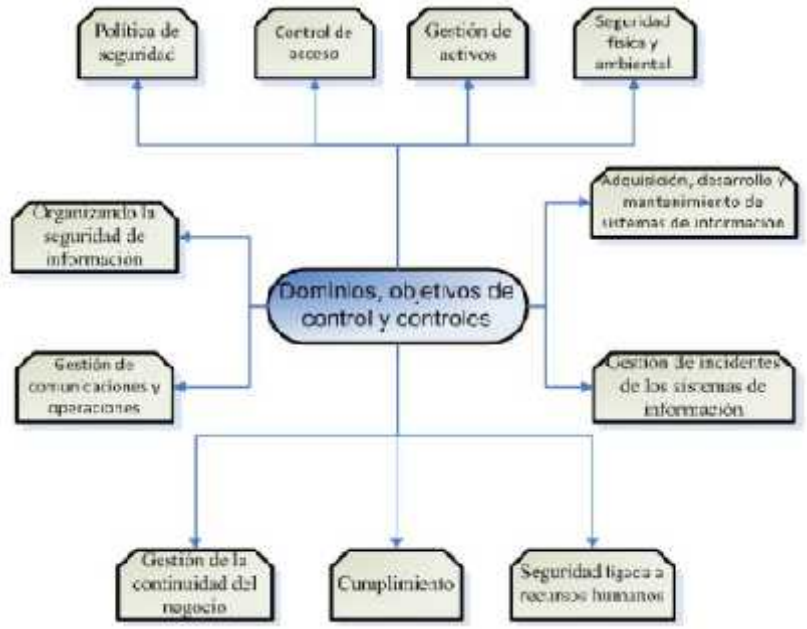


Figura 1.3 Dominios de ISO 27000

1.5.6. Dominio control de acceso

Del Peso (2004) define el control de acceso como “un mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.” [5]

Corletti (2006) afirma que “el control de acceso es una de las actividades más importantes de la arquitectura de seguridad de un sistema. Al igual que sucede en el mundo de la seguridad física, cualquiera que ha tenido que acceder a una caja de seguridad bancaria vivió como a medida que uno de llegando a áreas de mayor criticidad, las medidas de control de acceso se incrementan, en un sistema informático debería ser igual.” [6]

Los objetivos de control de este dominio se agrupan de la siguiente manera:

Tabla 2. Objetivos de control y controles del dominio [4]

Objetivo de control: Requisitos de negocio para el control de accesos	
Objetivo:	Controlar los accesos a la información.
Principios:	Se deberían controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización. Las regulaciones para el control de los accesos deberían considerar las políticas de distribución de la información y de autorizaciones.
Controles:	Política de control de accesos
Objetivo de control: Gestión de acceso de usuario	

Objetivo:	Gestión de acceso de usuario.
Principios:	Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información. Los procedimientos deberían cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información. Se debería prestar especial atención, si fuera oportuno, a la necesidad de controlar la asignación de permisos de acceso con privilegios que se salten y anulen la eficacia de los controles del sistema.
Controles:	Registro de usuario
	Gestión de privilegios
	Gestión de contraseñas de usuario
	Revisión de los derechos de acceso de los usuarios
Objetivo de control: Responsabilidades del usuario.	
Objetivo:	La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.
Principios:	Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su

	disposición. Se debería implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información.
Controles:	Uso de contraseña.
	Equipo informático de usuario desatendido.
	Políticas para escritorios y monitores sin información.
Objetivo de control: Control de acceso en red.	
Objetivo:	Impedir el acceso no autorizado a los servicios en red.
Principios:	Se deberían controlar los accesos a servicios internos y externos conectados en red. El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan: a) que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones; b) que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos; c) el cumplimiento del control de los accesos de los usuarios a los servicios de información.
Controles:	Política de uso de los servicios de red.

	Autenticación de usuario para conexiones externas.
	Autenticación de nodos de la red.
	Protección a puertos de diagnóstico remoto.
	Segregación en las redes.
	Control de conexión a las redes.
	Control de encaminamiento en la red.
Objetivo de control: Control de acceso al sistema operativo.	
Objetivo:	Impedir el acceso no autorizado al sistema operativo de los sistemas.
Principios:	Se deberían utilizar las prestaciones de seguridad del sistema operativo para permitir el acceso exclusivo a los usuarios autorizados. Las prestaciones deberían ser capaces de: a) la autenticación de los usuarios autorizados, de acuerdo a la política de control de accesos definida; b) registrar los intentos de autenticación correctos y fallidos del sistema; c) registrar el uso de privilegios especiales del sistema; d) emitir señales de alarma cuando se violan las políticas de seguridad del sistema; e) disponer los recursos adecuados para la autenticación;

	f) restringir los horarios de conexión de los usuarios cuando sea necesario.
Controles:	Procedimientos de conexión de terminales.
	Identificación y autenticación de usuario.
	Sistema de gestión de contraseñas.
	Uso de los servicios del sistema.
	Desconexión automática de terminales.
	Limitación del tiempo de conexión.
Objetivo de control: Control de acceso a las aplicaciones.	
Objetivo:	Impedir el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones.
Principios:	Se deberían utilizar dispositivos de seguridad con objeto de restringir el acceso a las aplicaciones y sus contenidos. Se debería restringir el acceso lógico a las aplicaciones software y su información únicamente a usuarios autorizados. Los sistemas de aplicación deberían: a) controlar el acceso de los usuarios a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida; b) proporcionar protección contra accesos no autorizados derivados del uso de cualquier

	utilidad, software del sistema operativo y software malicioso que puedan traspasar o eludir los controles del sistema o de las aplicaciones; c) no comprometer otros sistemas con los que se compartan recursos de información.
Controles:	Restricción de acceso a la información.
	Aislamiento de sistemas sensibles.
Objetivo de control: Informática móvil y tele trabajo.	
Objetivo:	Garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.
Principios:	La protección exigible debería estar en relación a los riesgos específicos que ocasionan estas formas específicas de trabajo. En el uso de la informática móvil deberían considerarse los riesgos de trabajar en entornos desprotegidos y aplicar la protección conveniente. En el caso del teletrabajo, la Organización debería aplicar las medidas de protección al lugar remoto y garantizar que las disposiciones adecuadas estén disponibles para esta modalidad de trabajo.
Controles:	Informática móvil.
	Tele trabajo.

CAPÍTULO 2

2. METODOLOGIA DE DESARROLLO DE LA SOLUCIÓN

2.1. Marco metodológico

2.1.1. Tipo de estudio

Para proceder a la creación del manual de políticas y normas de control de acceso necesitamos conocer usuarios y sistemas que tendrán acceso a la infraestructura de la compañía.

2.1.2. Tipo de investigación

- **Descriptiva:** Se procederá a observar y describir el comportamiento sin influir de ninguna manera.
- **Mixta:** Se procederá a usar un enfoque mixto para la revisión de procedimientos existentes y se procederá a realizar entrevistas a los usuarios de la compañía.

2.1.3. Método de investigación

- El método inductivo: Procederemos a investigar buenas prácticas para el control de acceso desde lo particular hasta lo general.
- El método científico: Se usará este método porque el manual resultante lo va a regir el dominio de control de acceso perteneciente a la norma ISO/IEC 27002:2005.

2.1.4. Fuentes y técnicas para la recolección de información

Entrevistas a usuarios:

Las entrevistas nos permitirán recoger información útil sobre los diferentes accesos y la información que se maneja.

Revisión de Documentación:

El departamento de TI de Impvet nos proporcionará la siguiente documentación para su correspondiente revisión:

- Documentación de políticas generales de TI.
- Documentación de políticas de sistemas para usuarios finales.
- Diagrama de diseño de la red de la compañía.
- Manual de usuario de los aplicativos.
- Manual de descripción de cargos (responsabilidades).

CAPÍTULO 3

3. ANALISIS Y PRESENTACIÓN DE RESULTADOS

3.1. Situación Actual

(Romo y Valarezo, 2012, pág. 32) afirman que “hoy en día la amenaza más importante contra nuestra información, la encontramos dentro de la misma empresa donde laboramos. Ya sea por accesos indebidos o no autorizados a la información corporativa son realizados principalmente por los empleados de la misma.” [6]

3.2. Diagnóstico

3.2.1. Análisis de las encuestas

Como se indicó en el Capítulo 2 del presente trabajo de investigación, se obtuvo información mediante entrevistas, y así se confirmó que no se mantienen normas de seguridad de la información, ni se aplican controles adecuados para el control de acceso. La entrevista con el

Jefe de Sistemas fue previa al desarrollo del manual resultante del presente trabajo de investigación, se realizaron preguntas cerradas teniendo en cuenta el dominio de control de acceso de la norma ISO 27002.

Tabla 3. Preguntas de la entrevista sobre el control de acceso

Pregunta	SI	NO	Observaciones
¿Se tienen políticas de control de acceso para las aplicaciones de la compañía Impvet Importadora Veterinaria Cía. Ltda.?			
¿Las políticas de control de acceso son aplicadas?			
¿Cuentan con un inventario actualizado para los accesos otorgados a los sistemas informáticos?			
¿Todas las aplicaciones que maneja Impvet Importadora Veterinaria Cía. Ltda. cuentan con una contraseña para permitir el acceso a los usuarios?			
¿Para el acceso remoto se tienen establecidos mecanismos de autenticación de usuarios a la red			

interna?			
¿Existen controles para monitorear los recursos de su compañía?			

El resultante de la entrevista muestra vulnerabilidades internas y/o externas, y concluye en el respaldo de la Gerencia para realizar el manual resultante de este trabajo de investigación.

3.3. Implementación de controles del dominio control de acceso (A.11).

En el presente trabajo de investigación se procede a detallar sólo los controles que se aplican a la infraestructura de la compañía Impvet Importadora Veterinaria. Cía. Ltda.

3.3.1. Requisitos del negocio para el control de acceso (A.11.1).

3.3.1.1. Política de control de acceso (A.11.1.1).

Control: "Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización." [4]

Lista de chequeo para implantación de políticas

1. Cada aplicativo de la compañía debe contar con un nivel de autenticación mínimo de usuario y contraseña como requisito de seguridad para el control de acceso.

2. Verificar la existencia de una política que obligue a mantener perfiles de acceso de los usuarios de la compañía.
3. Verificar la existencia de procedimientos para la actual administración de los accesos.
4. Verificar la existencia de procedimientos para el ingreso y salida de empleados de la compañía (usuarios).

Detalle las observaciones detectadas en la lista de chequeo

- No se encuentra actualizada la documentación respectiva de roles, responsabilidades y funciones de los usuarios en los aplicativos de la compañía y el acceso a los mismos.

3.3.2. Gestión de acceso de usuario (A.11.2).

3.3.2.1. Registro de usuario (A.11.2.1).

Control: "Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información." [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de un proceso para la socialización de las condiciones de acceso.

Detalle las observaciones detectadas en la lista de chequeo

- Existe un documento de responsabilidades y buenas prácticas para el uso de los aplicativos y los accesos a la red de la

compañía, sin embargo el mismo debe ser revisado y actualizado ya que la fecha de creación es mayor a 4 años.

3.3.2.2. Gestión de contraseñas de usuario (A.11.2.3).

Control: "Se debería controlar la asignación de contraseñas mediante un proceso de gestión formal." [4]

Lista de chequeo para implantación de políticas

1. Verificar la documentación referente a las políticas existentes para la administración de las contraseñas.
2. Verificar la existencia de un procedimiento para el cambio de las claves por defecto del hardware y software nuevo.
3. Verificar la existencia de un procedimiento para el manejo adecuado y sigiloso de las contraseñas de la compañía.

Detalle las observaciones detectadas en la lista de chequeo

- No existe un documento formal referente a las políticas para la administración de las contraseñas.
- No existe un procedimiento para el cambio de las contraseñas por defecto del hardware y software nuevo.

3.3.2.3. Revisión de los derechos de acceso de los usuarios (A.11.2.4).

Control: “El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.” [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de un procedimiento para la revisión periódica de los accesos de los usuarios y sistemas de la compañía.

Detalle las observaciones detectadas en la lista de chequeo

- No existe un procedimiento para la revisión periódica de los accesos. Se evidenció un documento de control de acceso y roles pero desactualizado y ya no funcional.

3.3.3. Responsabilidades del usuario (A.11.3).

3.3.3.1. Uso de contraseña (A.11.3.1).

Control: “Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas.” [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de políticas para el manejo de contraseñas por parte de los usuarios de la compañía.

Detalle las observaciones detectadas en la lista de chequeo

- Se confirma la existencia de un documento formal con respecto a las políticas de seguridad y buenas prácticas para el manejo de contraseñas por parte de los usuarios.

3.3.3.2. Equipo informático de usuario desatendido (A.11.3.2).

Control: "Los usuarios deberían garantizar que los equipos desatendidos disponen de la protección apropiada." [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de políticas para la protección de equipos en ausencia de sus usuarios.

Detalle las observaciones detectadas en la lista de chequeo

- Se confirma la existencia de políticas de dominio para la protección de los equipos desatendidos.

3.3.3.3. Políticas para escritorios y monitores sin información (A.11.3.3).

Control: "Políticas para escritorios y monitores limpios de información." [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de políticas para escritorios y monitores limpios de información.

Detalle las observaciones detectadas en la lista de chequeo

- No existe una política con respecto a escritorios y monitores limpios de información.

3.3.4. Control de acceso en red (A.11.4).

3.3.4.1. Política de uso de los servicios de red (A.11.4.1).

Control: “Se debería proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar.” [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de un procedimiento formal para la autorización de los accesos a la red de la compañía y sus servicios.

Detalle las observaciones detectadas en la lista de chequeo

- No existe un procedimiento para la autorización o revocación de accesos a la red y sus servicios.

3.3.4.2. Autenticación de nodos de la red (A.11.4.3).

Control: “Se debería considerar la identificación automática de los equipos como un medio de autenticación de conexiones procedentes de lugares y equipos específicos.” [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de un control que permita la identificación automática de equipos propios a la compañía y ajenos a la misma.

Detalle las observaciones detectadas en la lista de chequeo

- No existe un control que permita identificar los equipos propios de la compañía y los equipos ajenos a la misma. En caso que un equipo solicite una IP, el servicio DHCP procede a incluirla en la red interna.

3.3.4.3. Segregación en las redes (A.11.4.5).

Control: "Se deberían segregar los grupos de usuarios, servicios y sistemas de información en las redes." [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de segmentación de la red y segregación de grupos de usuarios y servicios en la red de la compañía.

Detalle las observaciones detectadas en la lista de chequeo

- Se confirma la existencia de un firewall de perímetro que controla los accesos no autorizados a la red interna.

3.3.4.4. Control de encaminamiento en la red (A.11.4.7).

Control: "Se deberían establecer controles de enrutamiento en las redes para asegurar que las conexiones de los ordenadores y

flujos de información no incumplen la política de control de accesos a las aplicaciones de negocio.” [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de políticas de control de encaminamiento en la red de la compañía.

Detalle las observaciones detectadas en la lista de chequeo

- No existe una política de control de encaminamiento en la red de la compañía.

3.3.5. Control de acceso al sistema operativo (A.11.5).

3.3.5.1. Procedimientos de conexión de terminales (A.11.5.1).

Control: “Debería controlarse el acceso al sistema operativo mediante procedimientos seguros de conexión.” [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de políticas de Directorio Activo referente al registro de accesos.

Detalle las observaciones detectadas en la lista de chequeo

- Se confirma la existencia de políticas de Directorio Activo referente al registro de accesos válidos y fallidos.

3.3.5.2. Sistema de gestión de contraseñas (A.11.5.3).

Control: “Los sistemas de gestión de contraseñas deberían ser interactivos y garantizar la calidad de las contraseñas.” [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de políticas de Directorio Activo referente a la gestión de contraseñas.

Detalle las observaciones detectadas en la lista de chequeo

- Buenas prácticas de seguridad de cuentas, máximo número de intentos fallidos, historial de contraseña, longitud de contraseña, complejidad de contraseña, cambio periódico de contraseña.

3.3.5.3. Uso de los servicios del sistema (A.11.5.4).

Control: “Se debería restringir y controlar muy de cerca el uso de programas de utilidad del sistema que pudieran ser capaces de eludir los controles del propio sistema y de las aplicaciones.” [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de políticas para el uso de cuentas administradoras.
2. Verificar la existencia de políticas para la instalación de servicios y aplicativos con elevación de privilegios.

Detalle las observaciones detectadas en la lista de chequeo

- Se confirma la existencia de políticas con respecto al uso de cuentas administradoras y su uso.

3.3.6. Informática móvil y tele trabajo. (A.11.7).

3.3.6.1. Informática móvil (A.11.7.1).

Control: “Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.” [4]

Lista de chequeo para implantación de políticas

1. Verificar la existencia de políticas de para el manejo de la informática móvil y telecomunicaciones.

Detalle las observaciones detectadas en la lista de chequeo

- No existen políticas ni procedimientos para el manejo de la informática móvil y telecomunicaciones.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Al finalizar el presente trabajo de investigación, análisis e implementación para el manual de políticas y normas de control de acceso para la empresa Impvet Importadora Veterinaria Cía. Ltda., concluyo resaltando los siguientes puntos que considero los más importantes:

1. Es responsabilidad del Departamento de TI de la compañía realizar el respectivo mantenimiento del actual manual de políticas y normas de control de acceso, su seguimiento y las adecuadas acciones correctivas y preventivas del mismo.

2. Es responsabilidad de los usuarios cumplir con el actual manual de políticas y normas de control de acceso.

3. La Gerencia de la compañía procederá a dar el soporte adecuado para la socialización y conciencialización del presente manual de políticas y normas de control de acceso.

4. El no cumplimiento de las políticas resultantes del presente trabajo de investigación deberá en parte ser revisado por el Departamento de TI y la Gerencia de la compañía para establecer sanciones respectivas de acuerdo al reglamento interno.

Recomendaciones

1. Se recomienda realizar campañas de socialización y concienciación de la importancia de la seguridad de la información tanto en el ámbito laboral como en la vida personal a todos los usuarios de la compañía.

2. La pronta implementación de un estándar de seguridad como la ISO 27000 para complementar los dominios restantes y la seguridad integral de la compañía.

3. Mantener el presente manual de políticas y normas de control de acceso siempre actualizado.

BIBLIOGRAFÍA

[1] Committee on National Security Systems (CNSS), National Information Assurance Glossary (CNSS Instruction No. 4009), http://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf, fecha de publicación 26 de abril de 2010

[2] Maya, E., & Jaramillo D., Auditoría de seguridad informática para el Gobierno Autónomo Descentralizado de Santa Ana de Cotacachi, basada en las normas NTP ISO/IEC 17799:2007 y la metodología OSSTMM v2., http://repositorio.utn.edu.ec/bitstream/123456789/3774/2/04%20RED%20034%20Art%C3%ADculo%20Cient%C3%ADfico%20Espa%C3%B1ol.pdf, fecha de consulta enero 2016

[3] Comité de Seguridad de la Información de la Universidad Técnica Nacional (Argentina), Políticas de Seguridad dela información – Plan de Acción 2009, http://www.utn.edu.ar/download.aspx?idFile=14736, fecha de consulta enero 2016

[4] aglone3, iso27002.es - El Anexo de ISO 27001 en español, https://iso27002.wiki.zoho.com/, fecha de consulta enero 2016

[5] Del Peso, E., El documento de seguridad (Análisis técnico y jurídico. Modelo), Ediciones Díaz de Santos, S.A., 2004

[6] Villafuerte, D. R., & Constante, J. V., Análisis e Implementación de la Norma ISO 27002 para el Departamento de Sistemas de la Universidad Politécnica Salesiana

Sede Guayaquil, http://dspace.ups.edu.ec/handle/123456789/3163, fecha de consulta enero 2016

ANEXOS

Anexo 1: Manual de políticas y normas de control de acceso.

El presente manual es el resultado del trabajo de investigación y análisis realizado en la compañía Impvet Importadora Veterinaria Cía. Ltda., es decir que el alcance de las políticas en él redactadas se encuentran sujetos a la realidad de la compañía. El presente manual tiene carácter de confidencial y se omitirá o cambiará nombres o configuraciones que comprometan la seguridad de la compañía.

1. DEL CONTROL DE ACCESO A LA RED Y SUS RECURSOS

1.1. Normas de acceso a la red y sus recursos

- El Departamento de TI debe establecer un procedimiento de autorización y controles para proteger el acceso a la red de datos y sus recursos.
- El Departamento de TI debe asegurar que la red inalámbrica de la compañía consta con métodos de autenticación que impida accesos no autorizados.
- La Gerencia debe autorizar la creación, modificación, bloqueo o eliminación de las cuentas de acceso a la red y/o sus recursos.
- El Departamento de TI debe establecer controles para la identificación y autenticación de los usuarios provistos por terceros en la red y/o sus recursos. Además estos usuarios deberán aceptar las responsabilidades previstas en las políticas de usuarios

finales de la compañía y recibir la charla de concienciación de la seguridad de la información.

- El Departamento de TI debe verificar periódicamente los controles de acceso para los usuarios provistos por terceros, con la finalidad de auditar que tengan acceso permitido sólo a los recursos de red y aplicativos para los que fueron autorizados.

2. DE LA ADMINISTRACIÓN DE ACCESO DE USUARIOS

2.1. Normas de administración de acceso de usuarios

- El Departamento de TI debe establecer un procedimiento formal para la administración de los usuarios en la red de datos, los recursos tecnológicos y los aplicativos de la compañía, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.
- El Departamento de TI debe definir lineamientos y buenas prácticas para la configuración de contraseñas que aplicaran sobre la infraestructura tecnológica, la red de datos y sus servicios y los aplicativos de la compañía. Estos lineamientos y buenas prácticas deben considerar aspectos como longitud, complejidad, control histórico, cambio cada cierto tiempo, bloqueo de cuenta por un número de intentos fallidos en la contraseña y cambio de la misma en el primer acceso, entre otros.
- El Departamento de TI debe asegurarse que los perfiles de usuario (usuarios y contraseñas) que vienen asignados por defecto en los

diferentes aplicativos y/o recursos de hardware sean modificados, inhabilitados o eliminados.

- La Gerencia debe autorizar la creación, modificación, bloqueo o eliminación de las cuentas de acceso a la red y/o sus recursos.

3. DE LAS RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

3.1. Normas de responsabilidades de acceso de los usuarios

- Los usuarios de la infraestructura tecnológica, la red y sus servicios y los aplicativos de la compañía deben hacerse responsables y ser conscientes de la seguridad de su usuario y contraseña.
- Los usuarios de la infraestructura tecnológica, la red y sus servicios y los aplicativos de la compañía deben hacerse responsables de las acciones realizadas en los mismos.

4. DEL USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACION

4.1. Normas de uso de altos privilegios y utilitarios de administración

- El Departamento de TI debe otorgar los privilegios para administración de la infraestructura tecnológica y sus recursos, de la red y sus servicios y de los aplicativos de la compañía sólo a aquellos funcionarios designados para dichas funciones.

- El Departamento de TI debe restringir las conexiones remotas a los recursos de la infraestructura tecnológica. Sólo se permitirá este acceso al personal debidamente autorizado, de acuerdo su perfil.
- El Departamento de TI debe establecer los controles necesarios para evitar que los usuarios finales o usuarios no autorizados tengan instalados en sus equipos software de alguna clase que permita accesos privilegiados.
- El Departamento de TI debe realizar el respectivo hardening de los sistemas operativos, aplicativos, el firmware, las bases de datos y el hardware de la infraestructura tecnológica de la compañía. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.
- El Departamento de TI debe procurar mantener actualizado y en un repositorio seguro un listado de las cuentas administrativas de los recursos de la infraestructura tecnológica.

5. DEL CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

5.1. Normas de control de acceso a sistemas y aplicativos

- El Departamento de TI debe establecer un procedimiento para la asignación del acceso a los sistemas y aplicativos de la compañía.
- El Departamento de TI debe establecer un ambiente de pruebas separado del ambiente de producción, con sus respectivas seguridades.

- El Departamento de TI debe establecer el procedimiento y los controles de acceso al ambiente de producción de los aplicativos de la compañía. Así mismo el procedimiento y los controles de acceso para las pruebas en el ambiente respectivo por parte de usuarios y/o desarrolladores internos y externos.
- El Departamento de TI debe verificar que los aplicativos desarrollados requieran autenticación mínimo de usuario y contraseña.
- El Departamento de TI debe verificar los aplicativos desarrollados no almacenen contraseñas, cadenas de conexión u otra información sensible en texto.