UNIVERSIDAD INTERNACIONAL SEK

DISEÑO DE UNA POLÍTICA PARA LA CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN BASADA EN RIESGOS PARA INSTITUCIONES PÚBLICAS EN EL ECUADOR

Ing. José Molina

MSc. Luis Fabián Hurtado Vargas

FORMULACIÓN DEL PROBLEMA

La institución pública que regula cooperativas y asociaciones, tiene la misión de supervisar y controlar su desempeño para garantizar el bienestar de todos los usuarios. Sin embargo, se ha detectado mediante el proceso de diagnóstico que existen inconsistencias en la gestión de la información; especialmente en jerarquización, accesibilidad y sistematización; evidenciando un nivel medio de vulnerabilidad lo cual afecta en la seguridad de todos los activos de información.

OBJETIVO GENERAL

Desarrollar una política para la clasificación y etiquetado de la información basado en riesgos, principalmente mediante el uso del conjunto de normas: ISO 27001:2013 y MAGERIT, posteriormente ISO 27002:2017 para generar mecanismos de control, con el fin de reducir considerablemente las inconsistencias en la gestión de la información de la institución encargada de regular cooperativas y asociaciones.

OBJETIVOS ESPECÍFICOS

- Elaborar un diagnóstico preliminar de la situación actual de la gestión de la información de la institución encargada de regular cooperativas y asociaciones mediante una metodología basada en entrevistas y análisis documental para identificar los riegos que existe en la institución.

- Realizar un levantamiento detallado de activos de la información de la institución encargada de regular cooperativas y asociaciones para desarrollar una política de clasificación y etiquetado que permitirá identificar el nivel de confiabilidad, integridad y disponibilidad de la información.

OBJETIVOS ESPECÍFICOS

- Evaluar las posibles amenazas y vulnerabilidades en los activos de la información ya organizado, para identificar el nivel de riesgo particular y así obtener una visión general del riesgo existente.

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Es una entidad técnica de supervisión y control que busca el desarrollo, estabilidad, solidez y correcto funcionamiento del sector económico popular y solidario sean esta financieras o no financieras con procesos técnicos, trasparentes y confiables, para contribuir el bienestar de sus integrantes y de la comunidad en general pensando en la satisfacción de las necesidades de las personas.

NORMAS, BUENAS PRÁCTICAS Y GUÍAS PROPUESTAS POR ORGANISMOS INTERNACIONALES

Magerit

Brinda un procedimiento frecuente para examinar los riesgos procedentes del empleo de medios tecnológicos de la información y comunicaciones (TIC)" (López, 2010, Pag. 21)

ISO/ IEC 27001/2013

Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI en el contexto de la organización. Además de especificar los requisitos para una evaluación y el tratamiento de los riesgos de seguridad de información adaptados a las necesidades de la organización.

ISO/ IEC 27002

fue creado con el objetivo de proporcionar la debida información a los responsables de la implementación de seguridad de la información. Es considerado como una buena practica para desarrollar y mantener normas de seguridad en una organización y así mejorar la confiabilidad de la seguridad de la información. En el que se define las estrategias de 133 controles de seguridad organizados bajo 11 dominios

DIAGNÓSTICO PRELIMINAR DE LA SITUACIÓN ACTUAL

Manejo de Reuniones y Entrevistas		
Fechas	Detalle	Conclusión
25/08/2017	Se respondió el oficio entregado para auspicio	Se obtiene carta de auspicio
29/08/2017	Presentación con el equipo de la dirección	Conocer el equipo de trabajo
01/09/2017	Reunión con el Director de Riesgos	Detección de riesgos en el manejo de la información.
05/09/2017	Entrevista con director de seguridad de la información en la que se trató sobre las necesidades que tiene la SEPS	Detección de vulnerabilidades
14/09/2017	Reunión con la experta en normativas donde se trató el manejo de la información actualmente y la visión a donde se quiere llegar	Detección del problema
28/09/2017	Reunión en la cual nos ayudó a responder preguntas y entender el manejo de la información dentro de la institución	se aclara el objetivo de la investigación
05/10/2017	Primera reunión para establecer procedimientos en levantamiento de activos	Realizar cronograma con los diferentes departamentos para levantamiento de activos

DEFINICIÓN DEL ALCANCE

- La institución cuenta con la dirección de seguridad de la información la cual se encarga de proteger los activos de información.
- La institución no cuenta con un sistema de gestión de seguridad de la información.
- No existe políticas de clasificación y etiquetado de la información que se genera y recopila dentro de la institución.
- No se utiliza metodologías para garantizar la confiabilidad, integridad y disponibilidad de los activos de la información.

DESARROLLO DE LA POLÍTICA PARA CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN BASADA EN RIESGOS

PLANIFICACIÓN

1.Definición del alcance

- Identificar la estrategia institucional - técnicas para recopilación de información.
- Especificar los sistemas de información que apoyan los procesos.
- Especificar los roles de los actores y sus responsabilidades

Definición de políticas de clasificación

- Definen las políticas de clasificación bajo qué criterios deben establecerse
- Etiqueta , valor/nivel identificando confidencialidad, integridad y disponibilidad.

1.Lineamientos a objetivos Institucionales

- La gestión de clasificación de información debe estar alineada al plan estratégico de la organización
- Identificar el alcance de que es lo que se va a identificar y clasificar

POLÍTICAS DE CLASIFICACIÓN

Tipo	Nivel / Valor	Confidencialidad	Integridad	Disponibilidad
TOP SECRET	5	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de servidores o funcionarios, generalmente de la alta dirección.	Información cuya modificación no autorizada no podría recuperarse, ocasionando pérdidas graves a la institución o a terceros. La pérdida de información puede conllevar un impacto negativo: • De índice legal o económica. • Retraso en sus funciones. • Pérdida de imagen severas de la entidad.	Información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la SEPS o a terceros. La no disponibilidad de la información puede conllevar a impactos negativos: • De índice legal o económica. • Retraso en sus funciones. • Pérdida de imagen severas a entes externos.
SECRETA	4	Información que sólo puede ser conocida y utilizada por un grupo de servidores o funcionarios. Es información crítica y solamente podrá ser conocida al interior de la Entidad ya que el conocimiento externo de la misma podrá ocasionar efectos negativos sobre la Entidad	Información cuya modificación no autorizada es de difícil recuperación y podría ocasionar pérdidas significativas para la institución o a terceros. La pérdida de información puede conllevar un impacto negativo: • De índice legal o económica. • Retraso en sus funciones. • Pérdida de imagen severas de la entidad.	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas a la institución o a terceros. podría ocasionar pérdidas significativas a la SEPS o a terceros. La no disponibilidad de la información puede conllevar a impactos negativos: • De índice legal o económica. • Retraso en sus funciones. • Pérdida de imagen moderado a entes externos.
CONFIDENCIAL	3	Información que puede ser conocida y utilizada por todos los servidores y funcionarios de la SEPS. Solo podrá ser accedida por grupos específicos de usuarios que requieren del conocimiento de esta información para estricto cumplimiento de sus funciones	Información cuya modificación no autorizada puede recuperarse aunque podría ocasionar pérdidas leves para la institución o a terceros. La información cuya modificación o eliminación puede ocasionar un impacto significativo dentro de las direcciones.	Información cuya inaccesibilidad permanente durante un mes o más, podría ocasionar pérdidas significativas para la institución o para terceros. La no disponibilidad de la información puede afectar a la operación normal pero no conlleva ampliaciones legales, económicas o pérdida de imagen.
RESTRINGIDA	2	Información que puede ser conocida y utilizada, sin autorización por cualquier persona. Podrá ser utilizada por todos los empleados directos de la SEPS y por empleados temporales, contratistas y/o terceros a la SEPS	Información cuya modificación no autorizada puede recuperarse fácilmente, o no afecta a la operatividad. La pérdida de información conlleva un impacto NO significativo para la entidad o entes externos	Información cuya inaccesibilidad no afecta la operatividad. La no disponibilidad de la información no conlleva implicaciones legales, ecuménicas o pérdida de imagen
PUBLICA	1	Información de disponible para cualquier persona externa a la institución. Información Publica	información que puede ser usado como informativa o material de investigación. Los activos de información que deben ser incluidos en el inventario como activos de información de integridad	Información que se encontrara publicada en medios digitales. La información puede acceder personas ajenas a la institución

IDENTIFICACIÓN Y CLASIFICACIÓN

Identificación	Pre clasificación de activos	Análisis de Riesgos
• Portafolio de servicios. • Inventario tecnológico • Procesos documentados	• Tipo de activo • Dimensión de valoración • Criterio de valoración	• El valor promedio de los tres valores asignados para cada activo de información determinará el valor de impacto general del activo. • Insignificante • Menor • Considerable • Grave • Supervivencia del negocio amenazada

CONFIDENCIALIDAD

Etiqueta	Descripción acuerdo confidencialidad
Top Secret	Información que sólo puede ser conocida y utilizada por un grupo muy reducido de servidores o funcionarios, generalmente de la alta dirección. información de alta importancia para la institución encargada de regular cooperativas y asociaciones que solo puede ser accedida por quienes ejerzan las funciones de: • Super Intendente • Directores
Secreta	Información que sólo puede ser conocida y utilizada por un grupo de servidores o funcionarios seleccionados. Es información crítica y solamente podrá ser conocida al interior de la Entidad ya que el conocimiento externo de la misma podrá ocasionar efectos negativos sobre la Entidad
Confidencial	Información que sólo puede ser conocida y utilizada por un grupo de servidores o funcionarios de una dirección o intendencia. Solo podrá ser accedida por grupos específicos de usuarios que requieren del conocimiento de esta información para estricto cumplimiento de sus funciones
Restringida	Información que puede ser conocida y utilizada por todos los servidores y funcionarios de la institución encargada de regular cooperativas y asociaciones. Podrá ser utilizada por todos los empleados directos y por empleados temporales, contratistas y/o terceros a la institución encargada de regular cooperativas y asociaciones
Pública	Información que puede ser conocida y utilizada sin autorización por cualquier persona. Información Publica

INTEGRIDAD

Etiqueta	Descripción acuerdo integridad
Top Secret	Información cuya modificación no autorizada no podría recuperarse, ocasionando pérdidas graves a la institución o a terceros. La pérdida de información puede conllevar un impacto negativo: • De índice legal o económica. • Pérdida de imagen severa de la entidad.
Secreta	Información cuya modificación no autorizada es de difícil recuperación y podría ocasionar pérdidas significativas para la institución o a terceros. La pérdida de información puede conllevar un impacto negativo: • Retraso en sus funciones. • Pérdida de imagen severas de la entidad.
Confidencial	Información cuya modificación no autorizada puede recuperarse, aunque podría ocasionar pérdidas leves para la institución o a terceros. La información cuya modificación o eliminación puede ocasionar un impacto significativo dentro de las direcciones.
Restringida	Información cuya modificación no autorizada puede recuperarse fácilmente, o no afecta a la operatividad. La pérdida de información conlleva un impacto NO significativo para la entidad o entes externos.
Pública	La información que puede ser usado como informativa o material de investigación. Los activos de información que deben ser incluidos en el inventario como activos de información de integridad.

DISPONIBILIDAD

Etiqueta	Descripción acuerdo disponibilidad
Top Secret	La información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas a la institución encargada de regular cooperativas y asociaciones o a terceros. La no disponibilidad de la información puede conllevar a impactos negativos: • De índice legal o económica. • Pérdida de imagen severas a entes externos.
Secreta	Información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas a la institución o a terceros. Podría ocasionar pérdidas significativas a la institución encargada de regular cooperativas y asociaciones o a terceros. La no disponibilidad de la información puede conllevar a impactos negativos: • Retraso en sus funciones. • Pérdida de imagen moderado a entes externos.
Confidencial	Información cuya inaccesibilidad permanente durante un mes o más, podría ocasionar pérdidas significativas para la institución o para terceros. La no disponibilidad de la información puede afectar a la operación normal pero no conlleva ampliaciones legales, económicas o pérdida de imagen.
Restringida	Información cuya inaccesibilidad no afecta la operatividad. La no disponibilidad de la información no conlleva implicaciones legales, económicas o pérdida de imagen
Pública	Información que se encontrara publicada en medios digitales La información puede acceder personas ajenas a la institución

VALORACIÓN DE ACTIVOS

Descripción	Cantidad	Tipo	Ubicación	Área	Propietario	Valoración Parcial			Valoración Final	Valor de Impacto
						C	D	I		
Archivo Word de la resolución con la finalidad de realizar la publicación en el registro oficial.	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Analista de Liquidación del Sector Financiero	3	4	4	4	Daño Grave
Documento de extracto de la resolución.	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Analista de Liquidación del Sector Financiero	1	1	3	2	Daño Menor
El archivo Word de la resolución tiene la finalidad de realizar la publicación en el registro oficial.	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Analista de Liquidación del Sector Financiero	2	2	4	3	Daño considerable
Convocatoria a calificación de acreencias para remitirlo a la Dirección Nacional de Comunicación.	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Analista de Liquidación del Sector Financiero	3	4	5	4	Daño Menor
Correo electrónico al analista de liquidaciones del sector financiero.	1	Software	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Analista de Liquidación del Sector Financiero	3	2	2	2	Daño Menor
El director recibirá y revisará el memorando y los artes adjuntos	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Director Nacional de Liquidación del Sector Financiero	3	2	2	2	Daño Menor
Correo electrónico a la prensa	1	Información	Matriz - Quito	Dirección de Liquidación del Sector Financiero	Director Nacional de Liquidación del Sector Financiero	2	1	1	1	Daño insignificante

POLÍTICA

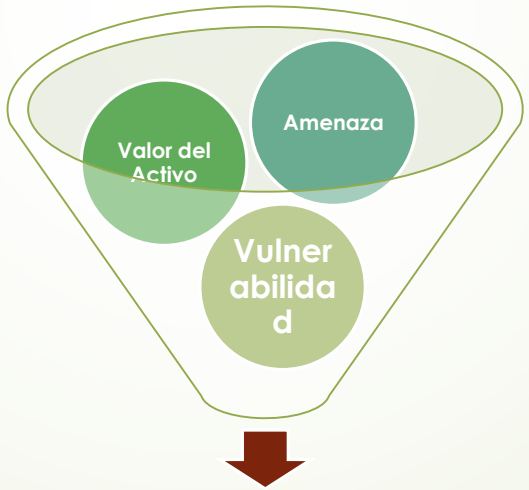
ACTIVO

CLASIFICACIÓN | ETIQUETADO

ANALISIS DE IMPACTO

DISPINIBILIDAD | INTEGRIDAD | CONFIABILIDAD

DETERMINACIÓN DE AMENAZAS Y VULNERABILIDADES



1.Nivel de riesgo

AMENAZAS

Nivel de Amenaza	Descripción	Justificación
3	La amenaza se considera presente y con alta probabilidad de que explote vulnerabilidades dentro del alcance.	No requiere
2	La amenaza se considera presente y con media probabilidad de que explote vulnerabilidades dentro del alcance.	No requiere
1	La amenaza se considera presente y con baja probabilidad de que explote vulnerabilidades dentro del alcance.	Requiere
0	La amenaza no está presente en el entorno del alcance de la implantación.	Requiere

VULNERABILIDADES

Vulnerabilidad	Descripción	Justificación
5	La vulnerabilidad ha sido explotada en el pasado, más allá del nivel de implantación del control.	No requiere
4	Es muy probable que la vulnerabilidad sea explotada en el futuro ya que el control no se ha implantado.	No requiere
3	Es probable que la vulnerabilidad sea explotada en el futuro, ya que el control se ha implantado parcialmente.	Requiere
2	Es poco probable que la vulnerabilidad sea explotada en el futuro, ya que el control está implantado.	Requiere
1	Es muy improbable que la vulnerabilidad sea explotada, ya que el control está implantado y auditado.	Requiere
0	La vulnerabilidad no aplica al activo, por lo que el control no se aplica.	Requiere

DETERMINACIÓN DEL NIVEL DE RIESGO

Valor del Activo X **Vulnerabilidad** = **Nivel de Riesgo**

Amenaza

Nivel de Amenaza		1					2					3				
Valor del Activo	Nivel de Vulnerabilidad	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
	1	1	2	3	4	5	2	4	6	8	10	3	6	9	12	15
	2	2	4	6	8	10	4	8	12	16	20	6	12	18	24	30
	3	3	6	9	12	15	6	12	18	24	30	9	18	27	36	45
	4	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60
	5	5	10	15	20	25	10	20	30	40	50	15	30	45	60	75
	Nivel de Riesgo															

Nivel de Riesgo	Descripción
1 – 24	No es necesario adoptar ninguna medida
25 – 48	Los riesgos que son aceptables o no a su juicio.
49 – 75	El nivel de riesgos no es aceptable,

1.Gestión del riesgo

- Aceptar el riesgo
- Tratar el riesgo
- Transferir el riesgo
- Evitar el riesgo

Riesgo residual

- Una vez aplicadas las medidas de control deberá situarse en un rango de valores por debajo del riesgo aceptable determinado por la empresa.

1.Revisión y monitorización

- El análisis de riesgo se repite con un intervalo anual, partiendo de los niveles de riesgo residual del análisis anterior.
- Se tiene que revisar el análisis de riesgos incluyendo
  - Cambios en la organización
  - Cambios tecnológicos.
  - Cambios en las amenazas.
  - Efectividad de los controles implantados.
  - Nuevos requisitos de seguridad de las partes interesadas.

Resultado del proyecto de investigación

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Quito 13 de junio del 2018

Señores
UNIVERSIDAD INTERNACIONAL SEK
Presente.

Asunto: "Finalización Proyecto"

De mis consideraciones:

Como es de su conocimiento el Ing. José Neptali Molina Alcocer portador de la cedula de identidad 1716454333, realizó su proyecto de tesis de la Maestría en Tecnologías de la Información con Mención en Seguridad de Redes y Comunicación denominado **"DISEÑO DE UNA POLÍTICA PARA LA CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN BASADA EN RIESGOS PARA INSTITUCIONES PÚBLICAS EN EL ECUADOR"** en la SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA, desde diciembre 2017 a junio 2018, el mismo que llegó a su etapa final cumpliendo los objetivos esperados por parte del maestrante.

De antemano agradecemos el tiempo y esmero que le dedico al proyecto

Sin otro particular me suscribo.

Atentamente,

Msg. Cristian Aguirre
Director Nacional de Seguridad de la Información
SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Av. Amazonas y Mariana de Jesús • www.seps.gob.ec •contactenos@seps.gob.ec • (593) 2 394 88 40

CONCLUSIONES

- Al desarrollar una política para la clasificación y etiquetado de la información basado en riesgos, se disminuyó considerablemente las inconsistencias en la gestión de la información de la institución encargada de regular cooperativas y asociaciones. La dirección de seguridad de la información expreso mediante un oficio su satisfacción por los resultados entregados con la investigación realizada.

- Se considera que la tecnología, procesos y las personas forman un trípode que sostienen la seguridad de la información: las instituciones públicas comúnmente cuentan con grandes presupuestos para la implementación tecnológica y definición de procesos, descuidando el talento humano y transformándose en el pilar más débil de la cadena de seguridad, por lo que es fundamental motivar a las personas que se integren en la cultura de la seguridad de la información.

RECOMENDACIONES

- Es importante conocer el proceso que se va analizar para realizar el levantamiento de activos de forma minuciosa dentro de la institución, detallando el nombre del activo, descripción, ubicación, propietario y tipo de activo, posteriormente se calificara el activo según su confiabilidad, integridad y disponibilidad con la colaboración del propietario del activo y responsables del proceso. Si el levantamiento de información es eficaz todo el proceso de evaluación de riesgo será satisfactorio.

- Se recomienda crear un comité de seguridad de la información el cual incrementará la protección de activos en la institución con políticas, gestión de los activos, seguridad de los recursos humanos, seguridad del entorno, control de accesos y gestión de los incidentes de la seguridad de la información.

MUCHAS GRACIAS