“DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA SWEADEN COMPAÑÍA DE SEGUROS S.A, BASADO EN LA NORMA ISO/IEC 27002:2013 ”

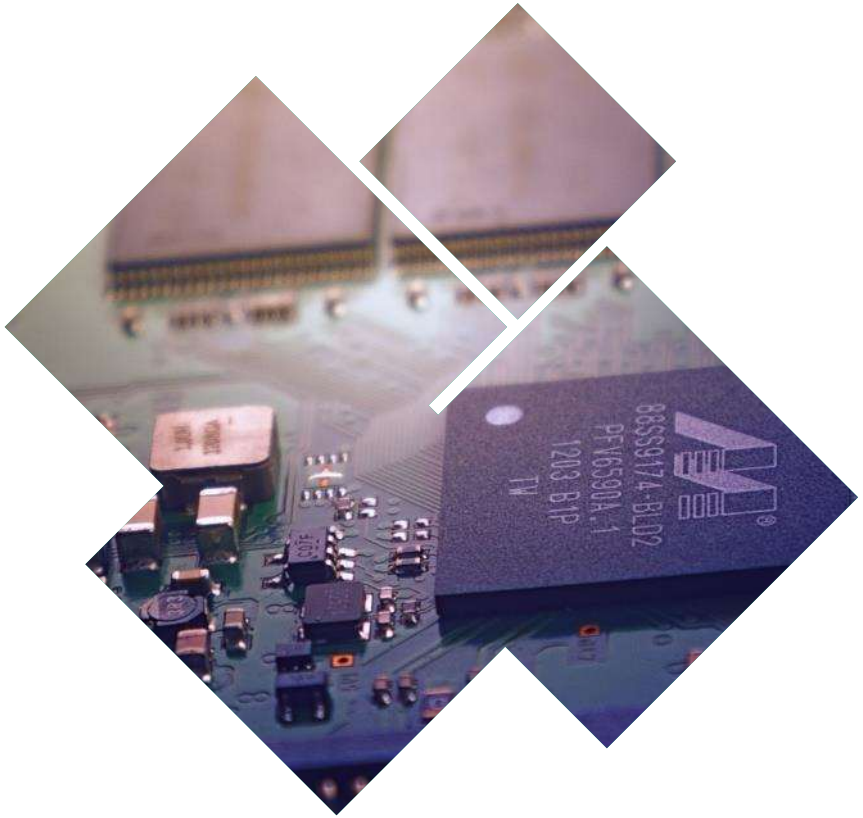
AUTOR: ANDRÉS ALMEIDA BAJAÑA

UNIVERSIDAD INTERNACIONAL UISEK

FACULTAD DE ARQUITECTURA E INGENIERÍAS

QUITO - 2019

CONTENIDO



1 Objetivos

2 Problema

3 Metodología

4 Resultados

5 Conclusiones y recomendaciones

Objetivos

GENERAL

Diseñar una política de seguridad de la información para SWEADEN COMPAÑÍA DE SEGUROS basada en la normativa ISO/IEC 27002:2013.

ESPECÍFICOS

01

02 Identificar la situación actual de la información de SWEADEN Seguros, mediante una matriz de riesgos basada en la metodología MAGERIT

03 Analizar el nivel de concientización en el manejo de seguridad y protección de la información que tiene el personal de la organización

04 Determinar los controles de la norma ISO/IEC 27002:2013 en base a la matriz de riesgos elaborada

05 Diseñar la política de seguridad para SWEADEN Seguros en base al análisis realizado a la norma ISO/IEC 27002:2013

PROBLEMA

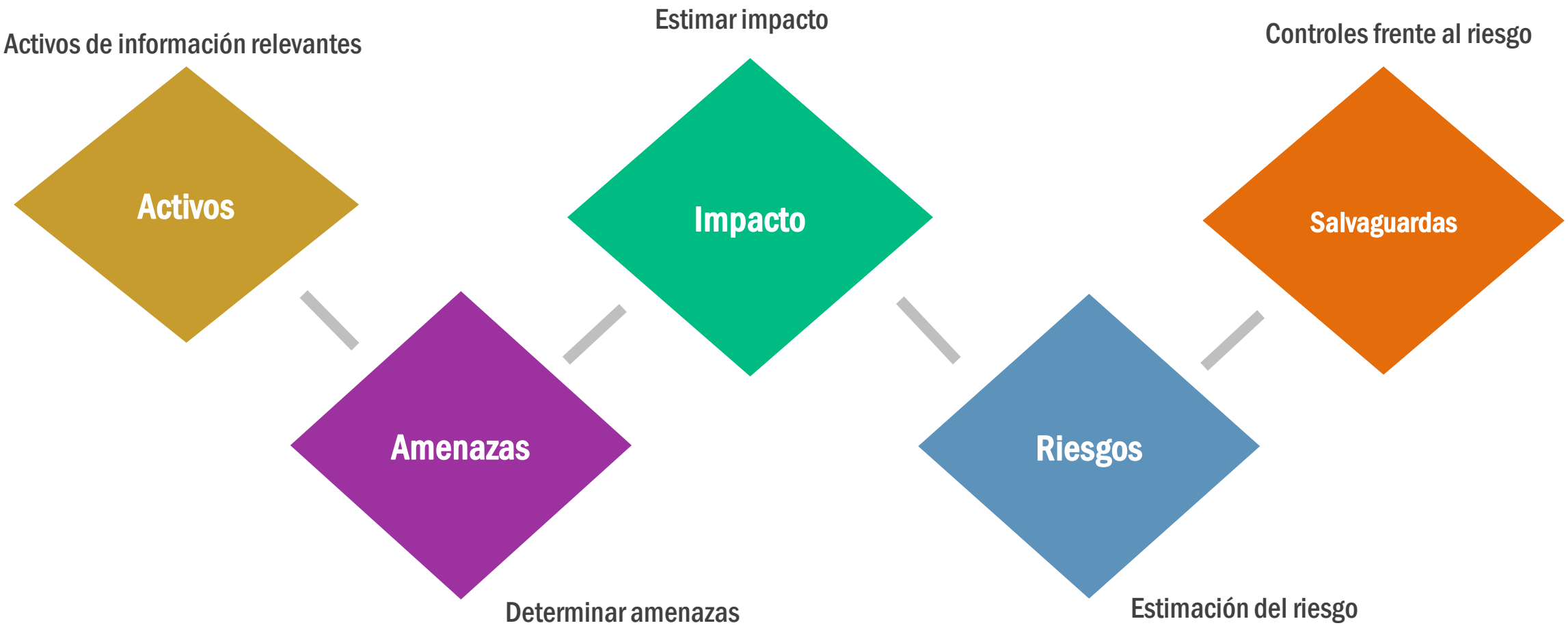
La falta de un SGSI para el area de TICS de SWEADEN SEGUROS manifestado en las siguientes situaciones:

- Control de acceso.
- Fuga de información.
- Planes de continuidad
- Falta de capacitación.
- Carencia de una política de seguridad de la información.

HALLAZGOS

1. La organización no cuenta con un sistema de Directorio Activo.
2. Se posee antivirus licenciado, pero existen equipos no protegidos.
3. El sistema web para asesores no posee certificado SSL.
4. El portal de consulta para facturación electrónica no posee certificado SSL.
5. Los usuarios que no hacen uso del bloqueo de pantallas.
6. Las credenciales de las cuentas de correos electrónicos de los usuarios son conocidas por los administradores de tecnología.
7. No existe puerta metálica ni con panel biométrico en el acceso al centro de cómputo.
8. Se evidencia que existe una deficiencia con el control de acceso a periféricos como USB.
9. No existen convenios de confidencialidad para las personas que ocupan cargos críticos.
10. El área de tecnología no posee una política de seguridad informática.

MAGERIT


Activos de información relevantes
Activos
Amenazas
Determinar amenazas
Estimar impacto
Impacto
Riesgos
Estimación del riesgo
Controles frente al riesgo
Salvaguardas

ESTIMACIÓN DE IMPACTO Y RIESGO

IMPACTO		*Degradación*				
		1%	10%	50%	90%	100%
		MB	**B**	**M**	**A**	**MA**
Probabilidad	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Elaborado por el investigador, basado en la metodología MAGERIT Libro III Versión 3, Pág. 6

RIESGO		*Probabilidad*				
		MB	**B**	**M**	**A**	**MA**
Impacto	**MA**			**RI17, RI22, RI47**	**RI27**	
	A		RI2, RI11, RI44	RI10, RI83, RI84		
	M		RI15, RI46, RI48, R53, R56, R57, R74, R78, R79, R82, R87, R90	R9, R34, R36, R45 R52, R54, R55, R58 R61, R62, R65, R66 R67, R69, R71, R72 R73, R76, R77, R80 R81, R85, R86		
	B	RI21, RI23, RI24, RI35	RI4, RI5, RI6, RI14, RI18, RI25, RI26, RI28, RI30, RI31, RI32, RI37, RI38, RI39, RI40, RI41, RI42, RI43 RI49, RI50, RI51, RI59, RI63, RI64, RI68, RI70, RI75, RI88, RI89, RI91, RI92	RI3, RI7, RI12, RI13, RI19, RI29, RI60	RI1	
	MB	RI8, RI16	RI20	RI33		

Fuente: Elaborado por el investigador

PROBLEMAS y SOLUCIONES

RIESGO

ISO 27002:2013

RI

12. Seguridad en la Operativa

12.1.1 Documentación de procedimientos de operación

[D] Código fuente de los Sistemas SIA, DIAMANTE, SISWEB.

2

[E.15] Alteración accidental de la información

A: Alteración accidental de la información.

V: Falta de control en la gestión del cambio.

Literal 96. El área de TICs debe establecer mecanismos seguros para la ejecución, monitoreo y control de copias de seguridad de la información crítica: Bases de datos, versionamiento del código fuente de los sistemas desarrollados.

PROBLEMAS y SOLUCIONES

RIESGO

RI

[D] Base Datos Sistemas: SIA, DIAMANTE, SISWEB

[E.2] Errores del administrador

A: Errores del administrador.

V: Falta de segregación de funciones.

10

ISO 27002:2013

12. Seguridad en la Operativa.

6. Aspectos organizativos de la seguridad de la información.

12.1.1 Documentación de procedimientos de operación.

6.1.2 Segregación de tareas.

Literal 93. Las bases de datos de la organización no deben ser manipuladas por ninguna circunstancia, de existir casos extraordinarios se debe aplicar el procedimiento de cambios en bases de datos luego de obtener la aprobación de la Alta Dirección y del coordinador de TICs además de ser una tarea ejecutada exclusivamente por el administrador de bases de datos.

PROBLEMAS y SOLUCIONES

RIESGO

RI

[D] Base Datos Sistemas: SIA, DIAMANTE, SISWEB

11

[E.15] Alteración accidental de la información

A: Alteración accidental de la información.

V: Falta de controles y privilegios en la DB.

ISO 27002:2013

9. Control de accesos.

9.1.1 Política de control de accesos.

9.2.2 Gestión de los derechos de acceso asignados a usuarios

Literal 47. Para garantizar el acceso autorizado a las redes y servicios informáticos, la organización debe contar con las herramientas que permitan gestionar correctamente el acceso, para ello es muy importante y obligatorio contar un controlador de dominio o directorio activo.

PROBLEMAS y SOLUCIONES

RI

[D] Base Datos Sistemas: SIA, DIAMANTE, SISWEB

[A.18] Destrucción de información

A: Destrucción de información.

V: Falta de controles en la gestión de respaldos.

12. Seguridad en la operativa.

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

12.3.1 Copias de seguridad de la información.

17.1.1 Planificación de la continuidad de la seguridad de la información.

17.1.2 Implantación de la continuidad de la seguridad de la información

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. (Redundancias)

17

Literal 133. La Alta Dirección de SWEADEN Seguros debe apoyar al área de TICs para la implementación de un Plan de Continuidad del Negocio BCP (Business Continuity Plan), con esto la organización podría reaccionar ante un incidente de seguridad permitiéndole restablecer sus operaciones de manera segura.

PROBLEMAS y SOLUCIONES

RI 22

12. Seguridad en la operativa.

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

12.3.1 Copias de seguridad de la información.

17.1.2 Implantación de la continuidad de la seguridad de la información.

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información. (Redundancias)

[D] NAS

RI 27

[E.18] Destrucción de información

A: Destrucción de información.

V: Falta de control en la segregación de privilegios.

[A.18] Destrucción de información

A: Destrucción de información.

V: Falta de controles en la gestión de respaldos.

Literal 132. La continuidad del negocio de las operaciones del área de TICs debe cumplir con los siguientes puntos:

- Identificación de los activos críticos a proteger.
- Elaborar el plan de continuidad del negocio y contingencias donde se establecerán los responsables y las responsabilidades de los usuarios.
- Se deberán realizar pruebas periódicas a los planes para garantizar su efectividad.
- Los planes de continuidad del negocio y contingencias siempre deberán estar actualizados.

PROBLEMAS y SOLUCIONES

RIESGO

RI 44

[SW] De desarrollo In House: SIA, DIAMANTE, SISWEB

[I.5] Avería de origen físico o lógico

A: Avería de origen físico o lógico.

V: Falta de controles en las pruebas del Software resultante.

[E.21] Errores de mantenimiento / actualización de programas (software)

A: Errores de mantenimiento / actualización de programas (software)

V: Falta de controles en la gestión del cambio

ISO 27002:2013

12. Seguridad en la Operativa.

14. Adquisición, desarrollo y mantenimiento de los sistemas de información

14.2.2 Procedimientos de control de cambios en los sistemas.

4.2.9 Pruebas de aceptación.

12.1.4 Separación de entornos de desarrollo, prueba y producción

RI 47

Literal 6. Para garantizar una adecuada gestión dentro del proceso de Desarrollo, SWEADEN Seguros debe segregar las funciones de tecnología habilitando responsables en cada fase del proceso, para ello se propone que existan:

- Coordinador de Desarrollo y QA
- Analistas Programadores
- Gestor de Base de datos

PROBLEMAS y SOLUCIONES

RIESGO

RI 83

[L] Datacenter

[A.11] Acceso no autorizado

A: Acceso no autorizado.

V: Falta de controles de seguridad física.

[A.23] Manipulación de los equipos

A: Manipulación de los equipos.

V: Falta de controles de seguridad física.

RI 84

ISO 27002:2013

11. Seguridad física y ambiental.

11.1.2 Controles físicos de entrada.

11.1.1 Perímetro de seguridad física.

Literal 76. El acceso a los sitios de procesamiento y almacenamiento de información exclusivamente los centros de datos deben poseer la seguridad física necesaria, esto quiere decir que deben brindar la seguridad contra accesos no autorizados, mediante el uso de mecanismos seguros que permitan la autenticación monitoreo y registro.

CONCLUSIONES

Usando la metodología MAGERIT se generó una matriz que permitió identificar los riesgos más críticos a los que se expone la información en SWEADEN, la ventaja de aplicar controles de la ISO/IEC 27002 es que permiten controlar dichos riesgos para mejorar la Confidencialidad, Integridad y Disponibilidad de la información.

01

Al no contar con una política de seguridad, el riesgo de los activos de información de las empresas aumenta considerablemente, dando cabida a las interrupciones de la operaciones del negocio de manera temporal o permanente.

02

SWEADEN Seguros posee brechas de seguridad en los siguientes dominios de seguridad: Seguridad en las operaciones, Continuidad del negocio, Control de accesos, Seguridad ambiental y física y Seguridad en los Procesos de Desarrollo.

03

Las ventajas de implementar los controles de la ISO 27002 y contar con una política formal de seguridad ayudan a que las empresas puedan: Generar conciencia sobre la seguridad de la información, Identificar y controlar riesgos asociados a la misma, preservar sus activos de información críticos, reduciendo de esta manera los problemas con la seguridad de la información.

04

RECOMENDACIONES

Se recomienda que la política de seguridad sea socializada con toda la organización.

01

la organización priorice e implemente los controles para la mitigación de los riesgos más críticos mencionados en la matriz de riesgo: Implementación de un controlador de dominio para controlar el acceso a la red y la implementación de los planes BCP y DRP de manera que se asegure la continuidad del negocio y sus operaciones.

02

La seguridad de la información no solo depende únicamente del diseño de la Política de seguridad propuesta, por lo que la implementación, evaluación y mejoramiento del plan de seguridad es una oportunidad muy recomendable para mejorar el aseguramiento de los datos.

03

“Los verdaderos hackers siguen un cierto conjunto de reglas éticas, que les impiden lucrarse o causar daño en sus actividades.”

KevinMitnick

Quito - Ecuador

(593) +995284856

jalmeida.mti@uisek.edu.ec

Gracias!