1 Objetivo y Alcance

Describir lo necesario para implementar el tratamiento de riesgos de seguridad y privacidad de la información en la Universidad de Pamplona.

2 Definiciones

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

NOTA Se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.[ISO/IEC Guía 73:2002]

Comunicación del riesgo: Intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.[ISO/IEC Guía 73:2002]

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.[ISO/IEC Guía 73:2002]

NOTA 1 En el contexto de esta norma, el término "actividad" se utiliza en lugar del término "proceso" para la estimación del riesgo.

NOTA 2 En el contexto de esta norma, el término "posibilidad" se utiliza en lugar del término "probabilidad" para la estimación del riesgo.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.[ISO/IEC Guía 73:2002]

NOTA En el contexto de esta norma, el término "actividad" se utiliza en lugar del término "proceso" para la identificación del riesgo.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.[ISO/IEC Guía 73:2002]

NOTA En el contexto de esta norma, el término "posibilidad" se utiliza en lugar del término "probabilidad" para la reducción del riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular. [ISO/IEC Guía 73:2002]

NOTA En el contexto de los riesgos en la seguridad de la información, únicamente se consideran las consecuencias negativas (pérdidas) para la retención del riesgo.

Transferencia del riesgo: Compartir con otra de las partes la pérdida o la ganancia de un riesgo.[ISO/IEC Guía 73:2002]

Confidencialidad: La información debe ser clara sólo para los extremos autorizados.

Integridad: La información no debe ser alterada durante el transporte por las redes inseguras.

Continuidad: La información debe estar disponible para los usuarios auténticos.

TCP/IP: Pila de protocolos implementado por la IETF que permite la implementación de redes WAN con conmutación de paquetes por medio de direccionamiento jerárquico usando direcciones IP y que logra el transporte confiable gracias a su manejo de errores usando TCP.

RFC: Request For Comments. Documento netamente técnico emitido por la IETF que define los detalles de un protocolo involucrado en la pila de protocolos TCP/IP.

IETF: Internet Engeenering T Force. La Fuerza de Trabajo de Ingeniería de Internet

Host: Un servidor, PC, estación de trabajo o dispositivo móvil que en algún momento posee una dirección de capa de red de la pila de protocolos TCP/IP.

NAT: Network Address Translation (Traducción de Direcciones de RED). Es cuando un firewall convierte una IP de origen en una IP de destino.

IPS: Intruder Prevention System. Un sistema preventor de intrusos que permite de acuerdo a parámetros de configuración emitir alarmas y en algunos casos acciones automáticas ante ataques reconocidos.

3 INTRODUCCIÓN

Debido al gran auge en el uso de las redes para la implementación de procesos y el transporte de información, toda institución debe mantener un análisis y gestión de riesgos de seguridad de la información efectivo que le permita afinar el esquema y lograr mejorar y tomar acciones ante hechos que de alguna forma debiliten la seguridad o amenacen alguno de elementos que caracterizan el esquema seguro.

La Universidad de Pamplona buscando implementar la ISO 27001, define esta gestión como parte esencial y obligatoria de esta norma y buscando cumplir con una amalgama con otros proveedores o clientes establece la forma de gestionar los controles recomendados por la ISO 27002. El Análisis y Gestión de Riesgos a realizar en la Universidad de Pamplona hará parte junto con otros documentos recomendados en la norma y creados de forma personalizada para la Universidad de Pamplona, y logrará de forma integral la implementación de la norma ISO 27001, también teniendo en cuenta que la Universidad de Pamplona ya cuenta con la certificación en ISO 9001 y la GP 1000.

El análisis y gestión del riesgo en la Universidad de Pamplona sigue al pie de la letra la metodología recomendada en la familia ISO 27000. Es así como inicialmente se identifican los activos, posteriormente se hace una estimación del riesgo, luego se sigue con la evaluación y finalmente con el tratamiento.

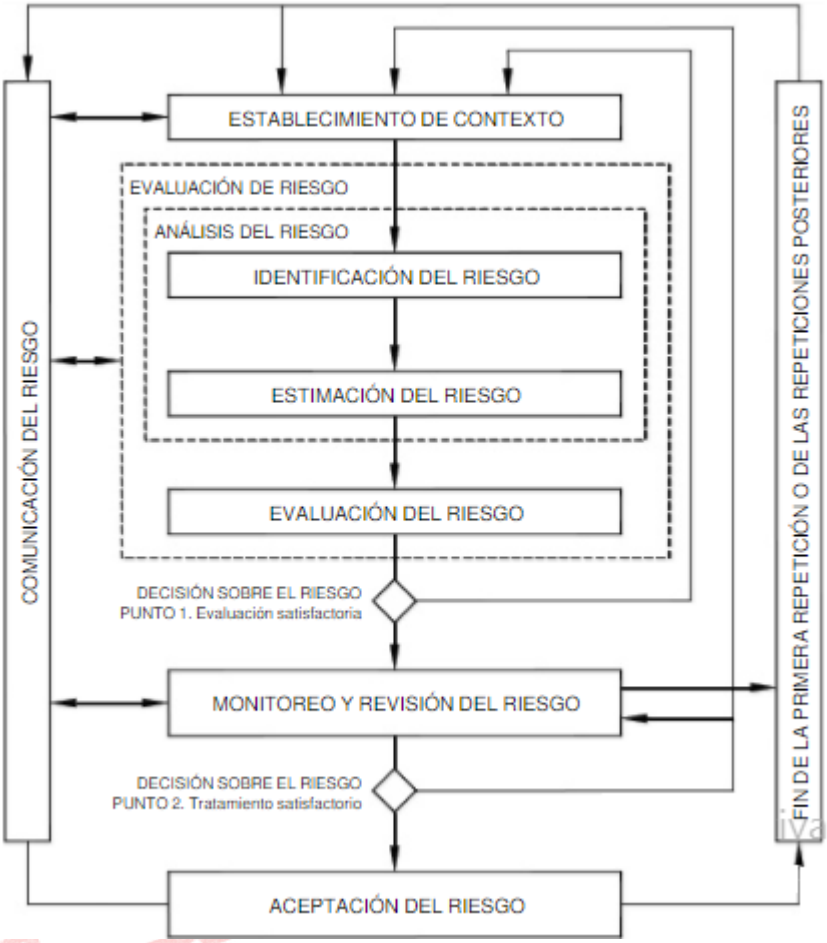

Figura 1. Proceso de gestión del riesgo en la seguridad de la información

Así como lo ilustra la Figura 1, el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o de tratamiento del riesgo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración. El enfoque iterativo suministra un buen equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, incluso garantizando que los riesgos altos se valoren de manera correcta.

El contexto se establece primero. Luego se realiza una valoración del riesgo. Si ésta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos hasta un nivel aceptable, entonces la labor está terminada y sigue el tratamiento del riesgo. Si la

información no es suficiente, se llevará acabo otra iteración de la valoración del riesgo con un contexto revisado (por ejemplo, los criterios de evaluación del riesgo, los criterios para aceptar el riesgo o los criterios de impacto), posiblemente en partes limitadas del alcance total (véase la Figura 1, Decisión sobre el riesgo-punto 1).

La eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual. En esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto (por ejemplo criterios para valoración del riesgo, de aceptación o de impacto del riesgo), seguida del tratamiento del riesgo (véase la Figura 1, Decisión sobre el riesgo-punto 2).

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la organización. Esto es especialmente importante en una situación en la que la implementación de los controles se omite o se pospone, por ejemplo debido al costo.

Durante todo el proceso de gestión del riesgo en la seguridad de la información es importante que los riesgos y su tratamiento se comuniquen a los directores y al personal operativo correspondiente. Incluso antes del tratamiento de los riesgos, la información acerca de los riesgos identificados puede ser muy valiosa para la gestión de incidentes y puede ayudar a reducir el daño potencial. La toma de conciencia por parte de los directores y el personal acerca de los riesgos, la naturaleza de los controles establecidos para mitigar los riesgos y las áreas de interés para la organización facilitan el tratamiento de los incidentes y los eventos inesperados de una manera más eficaz. Se recomienda documentar los resultados detallados en cada actividad del proceso de gestión del riesgo en la seguridad de la información y de los dos puntos de decisión sobre el riesgo.

La norma ISO/IEC 27001 especifica que los controles implementados dentro del alcance, los límites y el contexto de SGSI se deben basar en el riesgo. La aplicación de un proceso de gestión del riesgo en la seguridad de la información puede satisfacer este requisito. Existen muchos enfoques mediante los cuales se puede implementar exitosamente el proceso en una organización. La organización debería utilizar cualquier enfoque que se ajuste mejor a sus circunstancias para cada aplicación específica del proceso.

En un SGSI, el establecimiento del contexto, la valoración del riesgo, el desarrollo del plan de tratamiento del riesgo y la aceptación del riesgo son parte de la fase de "planificar". En la fase de "hacer" del SGSI, se implementan las acciones y los controles que son necesarios para reducir el riesgo hasta un nivel aceptable, de acuerdo con el plan de tratamiento del riesgo. En la fase de "verificar" del SGSI, los directores determinarán la necesidad de revisiones de las valoraciones y del tratamiento del riesgo a la luz de los incidentes y los cambios en las circunstancias. En la fase de "actuar", se llevan a cabo todas las acciones que son necesarias, incluyendo la aplicación adicional del proceso de gestión del riesgo en la seguridad de la información.

4 GESTIÓN DEL RIESGO

4.1 CONTEXTUALIZACIÓN

En la Universidad de Pamplona la siguiente será la forma de catalogar el riesgo:

Valores para probabilidad y riesgo

PROBABILIDAD	ALTA	3
	MEDIA	2
	BAJA	1
IMPACTO	ALTO	3
	MEDIO	2
	BAJO	1

Tabla 1. Valores para probabilidad y riesgo

Cálculo del riesgo (Entre más alto el valor del riesgo mayor la prioridad)

RIESGO (P*I)		I		
		A	M	B
P	B	3	2	1
	M	6	4	2
	A	9	6	1

Tabla 2. Cálculo del riesgo

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017

Adicionalmente, en la Universidad de Pamplona no se ignorarán riegos.

4.2 ANÁLISIS

La metodología para la gestión de riesgos en seguridad de la información para la Universidad de Pamplona, se ha hecho identificando de manera única el riesgo. Es así como en la siguiente tabla se identifican de manera inicial y única los riesgos, identificación que seguirá siendo usada en las demás etapas.

ACTIVOS				
Clase	Tipo	Subtipo	**ID**	**Descripción**
Primario	Información	Vital	**1**	**Funcionalidad principal:** Gestión académica.
Primario	Información	Vital	**2**	**BD académica Academusoft**
Primario	Información	Vital	**3**	**Archivo Físico**
Soporte	Hardware	Fijo	**4**	**Servidor web**
Soporte	Hardware	Fijo	**5**	**Servidor BD**
Soporte	Red	Periféricos	**6**	**Switch**
Soporte	Sitio	Zona	**7**	**DataCenter: Normas: estándar TIA-942**
Soporte	Personal	Operación/Mantenimiento	**8**	**Desarrolladores**
Soporte	Personal	Operación/Mantenimiento	**9**	**Infraestructura**
Soporte	Sitio	Comunicación	**10**	**Internet:** Velocidad: 20Mb
Soporte	Software	Sistema en línea(Aplicaciones de negocio,	**12**	**Sistema de información** Academusoft

		aplicación específica del negocio)		
Soporte	Software	Software de seguridad	**13**	Servidor web,Apache
Soporte	Software	Sistema operativo	**14**	S.O del servidor, aplicación.
Soporte	*Red*	*Arquitectura de la red*	***15***	Red de servicio del sistema de información

Tabla 3. Activos para AGR en la Universidad de Pamplona

VULNERABILIDADES Y AMENAZAS				
Riesgo	**ID**	**ACTIVO**	**VULNERABILIDAD (ANEXO D)**	**AMENAZA (ANEXO D)**
1	12	SISTEMA DE INFORMACIÓN	FECHAS INCORRECTAS	ERROR EN EL USO
2	12	SISTEMA DE INFORMACIÓN	TABLAS DE CONTRASEÑA SIN PROTECCIÓN	FALSIFICACIÓN DE DERECHOS
3	12	SISTEMA DE INFORMACIÓN	GESTIÓN DEFICIENTE DE LAS CONTRASEÑAS	FALSIFICACIÓN DE DERECHOS
4	12	SISTEMA DE INFORMACIÓN	HABILITACIÓN DE SERVICIOS INNECESARIA	PROCEDIMIENTO ILEGAL DE DATOS
5	12	SISTEMA DE INFORMACIÓN	FALTAS DE COPIAS DE SEGURIDAD	MANIPULACIÓN DE SOFTWARE
6	12	SISTEMA DE INFORMACIÓN	FALTA DE PROTECCIÓN FÍSICA DE LAS PUERTAS Y VENTANAS DEL EDIFICIO	HURTO A MEDIOS O DOCUMENTOS
7	13	SISTEMA DE INFORMACIÓN	TRAFICO SENSIBLE SIN PROTECCIÓN	ESCUCHA
8	14	SISTEMA DE INFORMACIÓN	HABILITACIÓN DE SERVICIOS INNECESARIOS	PROCEDIMIENTO ILEGAL DE DATOS
9	15	SISTEMA DE INFORMACIÓN	PERMITIVIDAD DE SERVICIOS	ACCESO INDEBIDO A SERVICIOS
10	16	SISTEMA DE INFORMACIÓN	DESACTUALIZACIÓN	EXPLOTACIÓN DE VULNERABILIDADES
11	13	SISTEMA DE INFORMACIÓN	DESACTUALIZACIÓN	EXPLOTACIÓN DE VULNERABILIDADES
12	11	SISTEMA DE INFORMACIÓN	DESACTUALIZACIÓN	EXPLOTACIÓN DE VULNERABILIDADES
13	8	SISTEMA DE INFORMACIÓN	EMTRENAMIENTO INSUFIENTE EN SEGURIDAD	ERROR EN EL USO

14	7	SISTEMA DE INFORMACIÓN	USO INADECUADO DEL CONTROL DE ACCESO FISICO AL RECINTO.	DESTRUCCION DE EQUIPO
15	12	SISTEMA DE INFORMACIÓN	FALTA DE LA TERMINACIÓN DE LA SESIÓN CUANDO SE ABANDONA LA SESIÓN DE TRABAJO	ABUSO DE LOS DERECHOS

Tabla 4. Vulnerabilidades y amenazas en la Universidad de Pamplona

4.3 ESTIMACIÓN

Riesgo	PROBRABILIDAD (P)	IMPACTO (I)	RIESGO (R*I)
1	2	2	4
2	3	3	9
3	3	3	9
4	3	3	9
5	3	3	9
6	3	3	9
7	3	3	9
8	3	3	9
9	3	3	9
10	3	3	9
11	3	3	9
12	3	3	9
13	3	3	9
14	3	3	9
15	3	3	9

Tabla 5. Estimación del riesgo en la Universidad de Pamplona

4.4 EVALUACIÓN

Riesgo	PROBRABILIDAD (P)	IMPACTO (I)	RIESGO (R*I)	PRIORIDAD
1	2	2	4	6
2	3	3	9	1
3	3	3	9	5
4	3	3	9	7
5	3	3	9	9
6	3	3	9	8
7	3	3	9	2
8	3	3	9	4
9	3	3	9	3

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017

10	3	3	9	7
11	3	3	9	7
12	3	3	9	7
13	3	3	9	6
14	3	3	9	3
15	3	3	9	3

Tabla 6. Evaluación del riesgo en la Universidad de Pamplona

4.5 TRATAMIENTO

Riesgo	CONTROLES ISO 27002	ACCIONES
1	12.4.1 Registro de Eventos	Sincronizar con NTP-SIC Colombia
2	12.6.1 Gestión de vulnerabilidades técnicas	Verificar coherencia e integridad de datos en las tablas de la BD.
3	10.1.2 Gestión de llaves: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida. 9.2.4 Gestión de acceso a usuarios 9.2.5 Revisión de los derechos de acceso de usuarios 9.3.1 Uso de información de autenticación secreta	Entregar formalmente los datos de identificación y autenticación a cada uno, definiendo, responsabilidades, citando la legislación y manifestando la información individual para la cual tome autorización. El sistema no debe permitir contraseñas inseguras. Obligar al cambio de contraseña periódicamente No permitir usar contraseñas históricas. El sistema tendrá un esquema: usuario-rol-funcionalidad, mediante el cual el rol define el tipo de acceso a la funcionalidad.
4	9.1.2 Eliminar los servicios de red innecesarios	Solo el usuario que ejecuta el motor tiene acceso de escritura a los archivos de la BD. El usuario que ejecuta la BD Tiene contraseña segura. La aplicación accede al motor por medio de un usuario que no es administrador y con clave segura. No se deben habilitar servicios que no se usen, por ejemplo en el administrador xampp activar solo los que se necesitan. MOD
5	12.3.a Copias de respaldo: se deberían	Se programaran el lapso de tiempo y frecuencia

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017

	producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados	en copias de seguridad.
6	11.1.6.c Áreas de despacho: las puertas externas de un área de despacho se deberían asegurar cuando las puertas internas están abiertas. 11.1.6.a El acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado	Se instalaran cámaras de seguridad en entradas y salidas. Se implementarán identificadores digitales para permitir el acceso a los recintos
7	9.1.2 Eliminar los servicios de red innecesarios	Se implementará un firewall para la protección del tráfico de datos.
8	9.4.3.h Almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicaciones 9.4.3.i Almacenar y transmitir las contraseñas en forma protegida.	Se calcula el HASH en el cliente y se compara con HASH de la tabla. El modelo de datos separa la tabla usuario de las de la aplicación
9	9.4.1.b Restricción de acceso a la información: controlar a qué datos puede tener acceso un usuario particular	Implementar un firewall de "filtrado de paquetes" - Definir política - Implementar reglas - VPN
10	12.6.1 Gestión de vulnerabilidades técnicas	Buscar una sincronización con el software utilizado y sus últimas versiones.
11	12.6.1 Gestión de vulnerabilidades técnicas	Verificar que el equipo este al día en actualizaciones cada lapso de tiempo.
12	12.6.1 Gestión de vulnerabilidades técnicas	Configurar para que se busquen automáticamente la disponibilidad de actualizaciones necesarias en el equipo.
13	12.6.1 Gestión de vulnerabilidades técnicas	Planificar reuniones o capacitaciones periódicamente.
14	11.1.2 Controles físicos de entrada	Instalación de cámara de seguridad y personal de vigilancia en lo posible.
15	9.4.2 Procedimiento de ingreso seguro	Cerrar sesión automáticamente después de cierto tiempo trascurrido sin actividad en la página o aplicación.

Tabla 7. Tratamiento del riesgo en la Universidad de Pamplona

5 Documentos de Referencia

Norma ISO 27001

Norma ISO 27002

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017

Norma ISO 27005

6 Historia de Modificaciones

Versión	Naturaleza del Cambio	Fecha de Aprobación	Fecha de Validación
0	Documento inicial	20/12/2017	20/12/2017

7 Anexo

“No aplica”.

Elaboró		Revisó
Jesús Evelio Ortega Arévalo		Avilio Villamizar Estrada
Fecha	20/12/2017	20/12/2017