Riesgos/vulnerabilidades de una red informática en un Laboratorio EDI

Fabián A. Gibellini, Roberto Muñoz, Analía L. Ruhl, Juliana Notreni, Milagros N. Zea Cárdenas, Ignacio Sánchez Balzaretti, Cecilia Sanchez

Laboratorio de Sistemas / Dpto. de Ingeniería en Sistemas de Información/
Universidad Tecnológica Nacional / Facultad Regional Córdoba
Maestro M. Lopez esq. Cruz Roja Argentina S/N, Ciudad Universitaria (X5016ZAA)-
Córdoba, Argentina
{fabiangibellini, robertmunioz, analialorenaruhl, julinotreni,
ignaciojsb, milyzc}@gmail.com, csanchezjuriol@hotmail.com

Resumen

La contribución de este trabajo es la presentación de un modelo de riesgos/vulnerabilidades de ciberseguridad en la red informática de un Laboratorio EDI. Este modelo permite ver la relación entre los riesgos/vulnerabilidades identificados y sus respectivos procesos de negocio. Además, el modelado muestra los riesgos más relevantes, categorización de riesgos, medidas de control para cada uno de los riesgos identificados. Estos riesgos/vulnerabilidades son el punto de entrada para identificar indicadores que serán comprendidos dentro las buenas prácticas de ciberseguridad.

Este estudio se realiza en la red informática de un Laboratorio EDI (Educación, Investigación y Desarrollo). Particularmente, es en el Laboratorio de Sistemas de Información (LabSis) de la Universidad Tecnológica Nacional Facultad Regional Córdoba. Los servicios brindados por el LabSis son diversos, y administra una red informática que da soporte a actividades académicas, actividades de investigación (I+D+I) y actividades de desarrollo de software.

Palabras claves: ciberseguridad, redes, infraestructura, procesos, riesgos, vulnerabilidades.

1 Introducción

Este estudio se encuentra inserto y forma parte del proyecto “Determinación de Indicadores, técnicas y herramientas que evidencian buenas prácticas en la ciberseguridad de la infraestructura tecnológica en un laboratorio de Educación, Investigación y Desarrollo de la UTN FRC”, homologado por la Secretaría de Ciencia y Tecnología bajo el código SIUTNCO0005366. Cuyo objetivo final es generar buenas prácticas en la ciberseguridad de la infraestructura tecnológica.

La línea de investigación estudiada es la ciberseguridad en redes de información y específicamente aplicada a la infraestructura de red de un Laboratorio de Educación, Investigación y Desarrollo (EDI).

Un Laboratorio EDI es un laboratorio donde diversas actividades deben convivir e incluyen necesidades y exigencias del día a día de actividades académicas, estudiantes, docentes, profesionales e investigadores.

Estas exigencias son cada vez mayores en lo que concierne a software, aplicativos y hardware. Es indispensable que este tipo de organización cuente con una infraestructura de red informática acorde para afrontar tales desafíos.

En el caso del Laboratorio de Ingeniería en Sistemas de Información (LabSis), de la Universidad Tecnológica Nacional Facultad Regional Córdoba (UTN-FRC) se atienden a todos los servicios de gabinete informático para actividades académicas, desarrollo de software y proyectos de investigación.

LabSis considera que sus servicios deben ser seguros, por lo que basándose en la disponibilidad, confidencialidad e integridad de los datos genera y busca generar mecanismos y procesos que ayuden a dar más seguridad a los datos. Entre los objetivos diarios que tiene que cumplir LabSis, se encuentran dar soporte académico a cátedras, soporte a la toma de exámenes y backup de los mismos [1], como así también dar soporte de infraestructura de red a proyectos de investigación como también generar nuevo software/configuración de software para suplir distintas tareas.

El presente trabajo está relacionado al trabajo presentado el año 2019 “Procedimientos de Seguridad en un Laboratorio EDI para la identificación de vulnerabilidades en su red informática.”, en el sentido que en el presente paper se pretende presentar un modelo de riesgos de ciberseguridad del Laboratorio EDI LabSis. [2]

Según la ISO/IEC 270001 es indispensable llevar a cabo acciones que den continuidad a los servicios, protegiendo la confidencialidad, integridad (autenticidad y no repudio de los datos) y disponibilidad de los mismos [3].

Consideraremos que este tipo de organización, no solo brinda servicios a un tipo de usuario sino a varios tipos de usuarios (alumnos, docentes, investigadores y desarrolladores) con necesidades muy distintas. En base a esto es crucial considerar la ciberseguridad [4] [5] de una red informática de este tipo de Laboratorio EDI, en parte a la diversidad de datos sensibles que se manipulan y en parte por la masividad de datos que se manejan.

Además, se tiene que tener en cuenta que ataques no solo provienen de atacantes externos sino también puede ser de atacantes internos, los cuales puede interrumpir la información, robar información, manipularla o incriminar al titular de la información en actos que este desconoce [6].

Por lo que sin una estrategia de ciberseguridad planteada no se podría medir ni controlar los incidentes relacionados a estos. Un estudio de IBM plantea que muchas organizaciones carecen de una clara y estrategia de seguridad alineada, tienen una visión limitada de su madurez de ciberseguridad y poseen practicar insuficientemente para responder a un incidente de ciberseguridad [7].

2 Metodología

En el desarrollo de este proyecto se utiliza el método empírico [8][9] para la observación, medición y análisis de los valores que sean obtenidos. La línea de investigación que se sigue es la ciberseguridad en redes de información, el objeto de estudio la red informática del Laboratorio de Ingeniería en Sistemas de Información (LabSis), de la Universidad Tecnológica Nacional Facultad Regional Córdoba (UTN-FRC). Este trabajo está conectado con "Procedimientos de Seguridad en un Laboratorio EDI para la identificación de vulnerabilidades en su red informática.", presentado en el CACIC 2019.

3 Desarrollo

Con el mapa de procesos y el detalle de cada uno de los procesos identificados llevó a cabo un análisis de riesgos del Laboratorio EDI.

Para el análisis de riesgos se establecieron tres categorías al riesgo según su tipo, estas son "Tecnico", de "Negocio" y de "Proceso".

- En el grupo de tipo Técnico se encuentran los riesgos relacionados a la calidad del servicio.
- Los riesgos de Negocio, los que afectan la viabilidad de la actividad.
- Los riesgos de Proceso a los que afectan a los procesos definidos por la organización.

Otra clasificación que se utilizó para los riesgos fue teniendo en cuenta su origen:

- Internos: aquellos que se originan dentro del contexto de la organización o son generados por personal de la misma
- Externos: que ocurren fuera del contexto de la organización es decir que es generada por un tercero.

Se identificaron los problemas realmente relevantes, o sea el 20% de los riesgos que tiene que te tener sí o sí un plan de contingencia [10]. De modo que, para identificar ese 20% de riesgos e idear un plan de contingencia para los mismos se determinó un nivel de exposición para cada uno. Se desarrolló una matriz de probabilidad en la que, primero, se precisó definir frecuencia, en base a valores históricos, como también su impacto para cada riesgo [11]. La frecuencia representa la probabilidad de que ese riesgo ocurra, teniendo como referencia incidentes históricos. El impacto indica el grado de afectación que tendría el laboratorio si ocurre el riesgo, en donde:

- "0" significa que no afecta
- "1" significa que el impacto afecta completamente a un servicio.

En base a esto se describieron cuatro niveles de exposición, "Bajo", "Tolerable", "Significativo" e "Intolerable", tal como se muestra en la Figura 1 (Fig. 1).

La determinación del nivel de exposición conduce al nivel de profundidad en la medida de contingencia que se tomará para cada riesgo. Por ejemplo si un riesgo posee un nivel de exposición Intolerable, se debe tener sí o sí un plan de contingencia que contemple al mínimo detalle como mitigarlo, en el caso que el riesgo ocurra. En cambio con un nivel de exposición bajo, a veces no es requerido un plan de contingencia para mitigar el mismo.

El nivel de exposición de todos los riesgos fue calculado a partir del producto de su frecuencia e impacto. La frecuencia de cada riesgo se determinó de forma empírica en base a hechos históricos.

Exposición	*Es necesario tomar medidas de control?*
Bajo	Riesgo entre 0.00 y 0.19. No es necesario tomar acción para abordar el riesgo
Tolerable	Riesgo entre 0.2 y 0.39. Evaluar si hay controles establecidos que hayan llevado el riesgo a tolerable y asegurar que se mantengan. No son necesarias medidas adicionales.
Significativo	Riesgo entre 0.4 y 0.6. Deben establecerse medidas de control para reducir el riesgo a Tolerable o Bajo. En caso que las medidas de control no sean inmediatas, se establecerán medidas transitorias.
Intolerable	Riesgos entre 0.61 y 1. La implementación de medidas de control debe ser inmediata. Las tareas no deberán comenzar o serán suspendidas hasta implementar las medidas de control.

Fig.1 Niveles de Exposición de Riesgos

Una vez definidos los criterios para el análisis de riesgo, se identificaron y analizaron las posibles amenazas que pueden intervenir en el correcto funcionamiento del Laboratorio EDI de LabSis.

A continuación se describen los procesos identificados

1. Administración de aulas
    1. Asignación anual/cuatrimestral de aula para cátedra
    2. Asignación y preparación de aula para parcial o examen
    3. Asignación de aula para práctica libre
    4. Asignación de aula por única vez para cátedra
2. Administración de usuarios
3. Preparación de nuevo equipamiento
4. Administración de software
    1. Mantenimiento de Software
    2. Instalación de software para cátedras
5. Administración de bases de datos
    1. Gestión de bases de datos para cátedras
    2. Gestión de bases de datos del LabSis
6. Administración de backups
    1. Gestión de backups del LabSis
    2. Gestión de backups para cátedras
7. Mantenimiento de hardware
8. Mantenimiento preventivo
9. Control de inventarios
10. Desarrollo de sistemas para el LabSis
11. Transferencia al medio
12. Investigación
13. Tutorías

Para estos procesos se identificaron los riesgos asociados los cuales sumaron un total de 35, podemos observar un resumen de dicho análisis (Fig. 2).

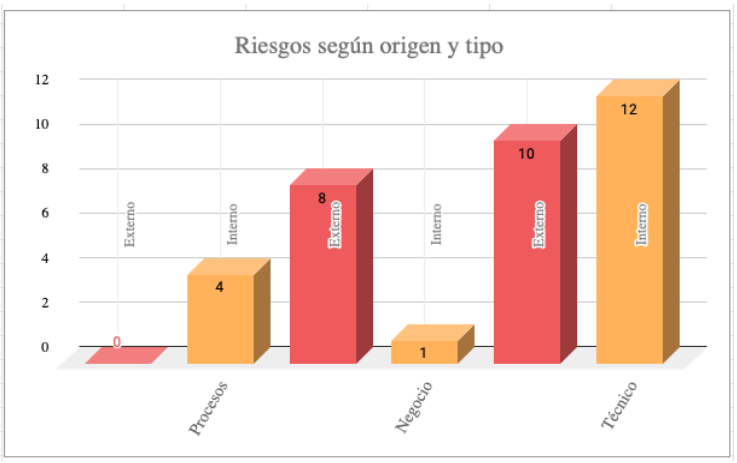

Fig.2 Cantidad de Riesgos según Origen y Tipo

Como podemos observar la mayoría de los riesgos identificados son técnicos. Por otro lado, todos los riesgos técnicos atentan contra la ciberseguridad de la red del LabSis ya que son consideradas vulnerabilidades que tienen que ser controladas y subsanadas.

En las Tabla 1, Tabla 2 y Tabla 3 se pueden ver los riesgos técnicos de exposición significativo o intolerable, es decir que si ocurren su impacto puede ser catastrófico. Por lo tanto si o si deben poseer medidas de control planificadas.

Tabla 1. Plan de contingencia riesgo R.19

ID	R.19
Amenaza	Inconsistencia en las versiones y configuraciones del software instalado en las aulas
Impacto	Imposibilidad de desarrollar la actividad académica por fallas de software o por no estar disponible la característica que se necesita. Imposibilidad de mover cursos entre aulas.
Frecuencia	0,6
Impacto	0,7
Exposición	0,42
Medidas de control	- Realizar una planilla que contenga por aula software instalado y versión - Actualizar aquellas aulas que se encuentran desactualizadas

Tabla 2. Plan de contingencia riesgo R.30

ID	R.30
Amenaza	No realizar pruebas de restauración de los backups almacenados
Impacto	Posibilita la falla de backups a la hora de recuperarlos y pérdida de datos
Frecuencia	0,8
Impacto	0,5
Exposición	0,4
Medidas de control	- Realizar capacitación de restauración de cada uno de los backup. - Realizar un instructivo con paso a paso de como realizar la restauración y posibles problemas que se pueden presentar.

Tabla 3. Plan de contingencia riesgo R.34

ID	R.34
Amenaza	No se cambian las contraseñas de los servidores periódicamente
Impacto	Posibilita la filtración de contraseñas que comprometan la seguridad de la infraestructura.
Frecuencia	0,9
Impacto	0,8
Exposición	0,72
Medidas de control	- Cambiar la contraseña cada vez que exista rotación de operadores.

Aunque para el presente se visualizan las medidas de control para los riesgos con nivel de exposición significativo o intolerable, para todo el estudio se identificaron medidas de control para todos los riesgos lo que permite.

4 Resultados, Avances/Discusión

Si bien los procesos descriptos fueron identificados para el LabSis, éstos pueden ser extrapolados a cualquier Laboratorio EDI. Como así también algunos de sus riesgos, con un previo análisis acorde a la adaptación de los procesos de cada laboratorio en particular.

El siguiente paso es identificar los indicadores que nos permitan monitorear y controlar estos riesgos/vulnerabilidades de la red del Laboratorio EDI de LabSis. Una vez identificados estos indicadores se procederá a la etapa de recolección de datos, los cuales generarán la base de conocimiento de indicadores de ciberseguridad de una red

informática. A partir de esta base de conocimiento de indicadores, se podrá determinar cuales serán considerados dentro las buenas prácticas de ciberseguridad

5 Referencias

[1] Dharma, R., Sake, S., Manuel, M. (2013). Backup and Recovery in a SAN. Versión 1.2. EMC2 Techbooks.
[2] (2017) A Comparison of Cybersecurity Risk Analysis Tools. Elsevier B.V.
[3] ISO/IEC 27001. "Tecnología de la información". Técnicas de la seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. ISO Ginebra, Suiza 2013
[4] (2008). UIT-T X. 1205. Serie X: Redes de Datos, Comunicaciones de Sistemas abiertos y seguridad. Ciberseguridad en el ciberespacio - Ciberseguridad. Aspectos generales de la ciberseguridad.
[5] What is cybersecurity?. CISCO. Recuperado de https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
[6] Harmantzis, F., Malek, M. (2004). Security Risk Analysis and Evaluation, IEEE Communications Society, pp. 1897-1901.
[7] (2020) Strategies for managing cybersecurity risk: Assess and advance your security and compliance posture. IBM Security. IBM Global Services
[8] Bunge, M. (1998). La ciencia su Método y su Filosofía. Editorial Siglo Veinte. Buenos Aires
[9] Barchini (2005). G. Métodos "I+D" de la Informática. Universidad Nacional de Santiago del Estero, Argentina
[10] Figueras A., Morero H., (2006) PARETO COMO CIENTÍFICO SOCIAL: A CIEN AÑOS DEL MANUAL. Asociación Argentina de Economía Política. Anales. Salta.
[11] (2017) Matriz de Riesgo, Evaluación y Gestión de Riesgos. SIGWEB. Página http://www.sigweb.cl/. Recuperado el 03/30/2020.