Indicadores de ciberseguridad de una red informática en un Laboratorio EDI

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

Laboratorio de Sistemas / Dpto. de Ingeniería en Sistemas de Información/
Universidad Tecnológica Nacional / Facultad Regional Córdoba
Cruz Roja Argentina S/N, 5016

fgibellini@bbs.frc.utn.edu.ar, robertmunioz@gmail.com, analialorenaruhl@gmail.com, csanchezjuriol@hotmail.com, julinotreni@gmail.com, milyzc@gmail.com, ignacio@bbs.frc.utn.edu.ar.

RESUMEN

El presente trabajo muestra los avances de la implementación del modelo de defensa de ciberseguridad en la infraestructura de red informática en un Laboratorio EDI.
Además, se presentan los riesgos relacionados a ciberseguridad y sus indicadores asociados. Dichos indicadores permitirán mitigar, contener o tomar acciones en un Laboratorio EDI.

***Palabras claves**: seguridad, redes, infraestructura, métricas, riesgo, indicadores.*

CONTEXTO

Este estudio está inserto y forma parte de un proyecto denominado "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.

1. INTRODUCCIÓN

Un Laboratorio de Educación, Investigación y Desarrollo (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, más ahora, en momentos de pandemia que, el laboratorio bajo estudio, brinda servicios a usuarios.
ITIL v3 define la seguridad de información como la protección activa de información, tanto almacenada como transportada, para asegurar que la misma está disponible sólo a los usuarios autorizados en el momento en que ellos la requieren, con los niveles apropiados de integridad [1].
El laboratorio objeto de estudio es el Laboratorio de Ingeniería en Sistemas de Información (LabSis), de la Universidad Tecnológica Nacional Facultad Regional Córdoba (UTN-FRC) y responde al concepto de un Laboratorio EDI.
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 [2], como así también dar soporte de infraestructura de red a proyectos de investigación, además de

generar nuevo software/configuración de software para suplir distintas tareas.
Según la ISO/IEC 270001 es esencial llevar a cabo ciertas acciones que den continuidad a los servicios, protegiendo la confidencialidad, integridad (autenticidad y no repudio de los datos) y disponibilidad de los mismos [3].
En cuanto a la ciberseguridad, Cisco [26] la define como la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ataques son dirigidos generalmente para acceder, cambiar o destruir información sensible; extorsionar por dinero a usuarios; o interrumpir el proceso normal de negocio. Por lo que implementar medidas efectivas de ciberseguridad es un desafío particular hoy en día porque hay más dispositivos que personas, y los atacantes se han vuelto más innovadores [4].
En base a la cantidad de datos que maneja el Laboratorio EDI en cuestión, es crítico considerar la ciberseguridad de su red informática, en parte también por la diversidad de datos sensibles que manipula, teniendo en cuenta que los servicios que debe prestar esta entidad a docentes y la protección de datos sensibles (entre ellos, los parciales y exámenes finales) cuya incumbencia concierne únicamente a la Universidad en que se realiza [5] [6].
Sumado a ello, se tiene que tener en cuenta que los ataques no sólo provienen de atacantes externos, sino también puede ser de atacantes internos, los cuales puede interrumpir procesos cruciales referentes a la información, robar información, manipularla o incriminar al titular de la información en actos que éste desconoce [7].
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 adecuada estrategia de seguridad alineada, tienen una visión limitada de su madurez de ciberseguridad y poseen prácticas insuficientemente para responder a un incidente de ciberseguridad [8].
En el presente trabajo se describen los riesgos relacionados a ciberseguridad y sus indicadores asociados. Este trabajo está relacionado con un modelo de defensa presentado durante el año 2019.

2. LÍNEAS DE INVESTIGACIÓN

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 (Laboratorio EDI).
En el desarrollo de este proyecto se utiliza el método empírico [9] [10], ya que los indicadores seleccionados, para su posterior recolección, fueron elegidos de forma empírica, teniendo en cuenta la historia del laboratorio y experiencias previas.
El estudio llevado a cabo en el LabSis, confluye sobre la seguridad informática en redes de información que operan sobre infraestructuras tecnológicas de un ámbito público, lo que podría aplicarse a otro ambiente de similares características.
Se llevó a cabo un análisis de riesgos [11], haciendo hincapié en los riesgos de ciberseguridad pero sin olvidar considerar otros tipos de riesgos. Luego se definieron indicadores o métricas [12] que nos permiten tener monitoreo y seguimiento de dichos riesgos
Los indicadores presentados en este trabajo son algunos del total identificado hasta este momento. Estos indicadores fortalecerán la seguridad de la red informática del Laboratorio EDI.

3. RESULTADOS OBTENIDOS/ESPERADOS

Para tener una visión global de todos los procesos/procedimientos de un Laboratorio EDI, procedimos a listar los procesos identificados en el LabSis:

1. Administración de aulas
    a. Asignación anual/cuatrimestral de aula para cátedra
    b. Asignación y preparación de aula para parcial o examen

   c. Asignación de aula para práctica libre
   d. Asignación de aula por única vez para cátedra
2. Administración de usuarios
3. Preparación de nuevo equipamiento
4. Administración de software
   a. Mantenimiento de Software
   b. Instalación de software para cátedras
5. Administración de bases de datos
   a. Gestión de bases de datos para cátedras
   b. Gestión de bases de datos del Labsis
6. Administración de backups
   a. Gestión de backups del LabSis
   b. 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, a través de un análisis de riesgos. El total de riesgos identificados fue de 35, podemos observar un resumen de dicho análisis (Figura 1).

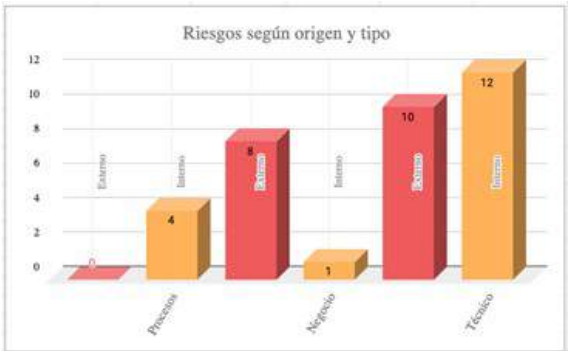

Figura 1. Cantidad de Riesgos según Origen y Tipo

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.
Cada uno de los riesgos identificados tiene un nivel de exposición (Figura 2), cuyo criterio fue definido antes del análisis de riesgos.

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 iniciarse o serán suspendidas hasta implementar las medidas de control.

Figura 2. Criterios de exposición de riesgos

La exposición de un riesgo es el producto entre las ponderaciones dadas al impacto y su frecuencia de ocurrencia. 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 las Tabla 1 y Tabla 2 se pueden ver algunos riesgos técnicos con una exposición significativa o intolerable, es decir que si ocurren su impacto puede ser catastrófico. Por lo tanto si o si deben poseer medidas de control planificadas

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	- Realizar capacitación

 RedUNCI - UNdeC. ISBN: 978-987-24611-3-3

control	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 1. Descripción de riesgo R.30

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.

Tabla 2. Descripción de riesgo R.34

Además, se identificaron:

- Riesgos que pueden ser mitigados con procedimientos.
- Riesgos que pueden ser mitigados mediante acciones administrativas que corrijan o mejoren la infraestructura.
- Riesgos que no se pueden mitigar ya que interfieren con el funcionamiento del Laboratorio EDI pero pueden ser monitoreados para reducir los posibles abusos.
- Riesgos que no pueden ser mitigados debido al costo o a la infraestructura y deben ser asumidos.

Como mencionamos antes, los riesgos técnicos son también riesgos de ciberseguridad, para estos riesgos se identificaron que permitan dar seguimiento a los riesgos, para poder tomar acciones preventivas o en el peor de los casos correctivas.

Los indicadores son valores muy disímiles entre sí ya que deben poder ser utilizados para evaluar la incidencia de los riesgos y los riesgos son por naturaleza distintos entre sí. Para esta selección de indicadores, se prioriza que sus valores se generen de forma automática y no dependan de una persona para confeccionarlos, es decir que los indicadores tengan una recolección automática.

Teniendo en cuenta todos los riesgos y principalmente los técnicos que atentan contra la ciberseguridad de la red del LabSis, un ejemplo de riesgo es el uso indebido de equipo, y su indicador asociado es el acceso a internet fuera de los horarios habilitados, para lo cual pueden generarse distintos eventos según sea el origen, el destino y el tipo de tráfico y en el caso en particular que se trata los eventos reflejan una cantidad en el tiempo por lo que pasado el tiempo de muestreo si el incidente persiste se generarán más eventos.

Los indicadores seleccionados se encuentran categorizados:

1. *Indicadores de Monitoreo de suministro eléctrico*: Permitirán autonomía eléctrica durante los cortes de luz
    a. Cantidad de cortes
    b. Duración de los cortes
2. *Monitoreo de las condiciones ambientales de los servidores*: Funcionamiento normal o anormal que requiere mantenimiento.
    a. Temperatura ambiente
    b. Temperatura de los servidores

 RedUNCI - UNdeC. ISBN: 978-987-24611-3-3

3. *Indicadores de Monitoreo del tráfico de red*: Para detectar tráfico de red anómalo
    a. Cantidad de conexiones /seg
    b. Cantidad de tráfico /seg
    c. Tráfico fuera de horario
    d. Tráfico a puertos o destinos inusuales
4. *Indicadores de Monitoreo de red*: Para detectar equipos posiblemente no autorizados dentro de la red. También para detectar equipos posiblemente no autorizados dentro de la red que estén extrayendo o ingresando datos o aplicaciones no autorizadas.
    a. Conexión de equipamiento de terceros
    b. Suplantación de IP de un equipo
    c. Detección de VMs con acceso directo a la red fuera de horario
5. *Indicadores de Monitoreo de equipos*:
    a. Uso de disco: Es necesario asegurar el uso de disco para los backup, toma de exámenes y correcto funcionamiento de equipo.
    b. Uso de memoria: Para asegurar el correcto funcionamiento de aplicaciones y VMs
    c. Programas sospechosos: Para evitar posibles fugas o daños de datos.
    d. Intento de elevación de privilegios: Para alertar de actividades sospechosas.
6. *Indicadores de Monitoreo de Usuarios*:
    a. Intentos de session con clave incorrecta: Para detectar comportamiento anómalo o ataques.
    b. Uso de usuarios distintos durante exámenes: Para detectar intentos de copia o uso indebido del sistema.
    c. Intentos de conexión remota: Para detectar intentos de copia o uso indebido del sistema

Por heterogeneidad se entiende que la unidad de medición de cada indicador es distinta y depende de lo que este cuantificando dicho indicador, podemos encontrar indicadores de cantidad en un tiempo dado, cantidad de conexiones por minuto, otros, tienen su unidad de medida del tipo absoluto como temperatura.

Además de los indicadores de recolección automática también existen indicadores de recolección manual, como por ejemplo el indicador asociado al riesgo "No se cambian las contraseñas de los servidores periódicamente" (R. 34) requiere un control manual para la verificación del cambio de contraseña para todos los involucrados.

Se determinó que es alta la complejidad de generar indicadores automáticos para los riesgos que se pueden mitigar con procedimientos.

Como conclusiones, respecto a los riesgos identificados en el análisis de riesgos, si bien su implementación fue en el Laboratorio de Sistemas, son extrapolables a cualquier Laboratorio EDI. Siempre considerando un análisis de revisión y/o adaptación previo.

Si bien los indicadores presentados tienen potencialidad de cubrir varios riesgos puede que algunos sean considerados rechazados o refutados durante la evaluación de los mismos, posterior a la etapa de recolección.

Dentro de los pasos a seguir están los de recolección de datos de los indicadores planteados lo que permitirá determinar su aceptación o rechazo como punto de referencia para mantener la red informática contenida o alerta ante cualquier anomalía o ataque.

4. FORMACIÓN DE RECURSOS

El grupo está compuesto por un Director, Co-Director, por investigadores de apoyo, profesores aspirantes a incorporarse a la carrera de investigador, técnicos de soporte, un estudiante investigador de la carrera de Ingeniería Electrónica y becarios que forman

parte del equipo. Este proyecto contribuirá a la formación y crecimiento de la carrera de los integrantes del mismo. En el caso de los estudiantes y algunos integrantes se iniciarán en la línea de seguridad informática.

5. BIBLIOGRAFÍA

[1] ITIL. Information Technology Infrastructure Library. Vs. 3 - 2001.
[2] Dharma, R., Sake, S., Manuel, M. (2013). Backup and Recovery in a SAN. Versión 1.2. EMC2 Techbooks
[3] ISO/IEC 27001. "Tecnología de la información". Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. ISO Ginebra, Suiza 2013.
[4] What is cybersecurity? CISCO.Recuperado de https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.
[5] (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.
[6] What is cybersecurity?. CISCO. Recuperado de https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.
[7] Harmantzis, F., Malek, M. (2004). Security Risk Analysis and Evaluation, IEEE Communications Society, pp. 1897-1901
[8] (2020) Strategies for managing cybersecurity risk: Assess and advance your security and compliance posture. IBM Security. IBM Global Services.
[9] Bunge, M. (1998). La ciencia su Método y su Filosofía. Editorial Siglo Veinte. Buenos Aires
[10] Barchini (2005). G. Métodos "I+D" de la Informática. Universidad Nacional de Santiago del Estero, Argentina.
[11] Lavanya, N. & Malarvizhi, T. (2008). Risk analysis and management: a vital key to effective project management. Paper presented at PMI® Global Congress 2008—Asia Pacific, Sydney, New South Wales, Australia. Newtown Square, PA: Project Management Institute.
[12] Hauser, John & Katz, Gerry. (1998). Metrics: You are what you measure!. European Management Journal. 16. 517-528. 10.1016/S0263-2373(98)00029-2.