Conclusiones

Haber implementado el esquema de seguridad dentro del Colegio de Ciencias y Humanidades, representó una experiencia enriquecedora en nuestro desarrollo profesional, después de haber realizado un análisis de las necesidades del Colegio en cuanto a seguridad de la información. El enfoque de protección que se plantea, con base en los objetivos, se centra en el diseño e implementación de un esquema de seguridad perimetral, punto que fue cubierto. Es importante destacar que gracias a este trabajo fue posible implementar el primer esquema de seguridad de red perimetral para la institución, esperando que las perspectivas de seguridad plasmadas en este documento presente al lector la importancia de la seguridad de la información, procedimientos, buenas prácticas y mecanismos que permitan llevar a cabo un ciclo de mejora continua.

El trabajo realizado en conclusión cumplió con los objetivos propuestos, considerando riesgos residuales aceptados por la dirección, a los cuales en un futuro se recomienda dar su adecuado tratamiento, mencionados en el tema 4.1. Dentro de los beneficios generados con este trabajo, considerando etapas de análisis, desarrollo del esquema e implementación, se listan las siguientes aportaciones:

- Un primer análisis de riesgos con base en el NIST 800-30, a través de los cuales se determinaron activos, amenazas, riesgos, así como controles para reducir la posibilidad de presentarse un incidente de seguridad, permite ser un punto inicial para futuros análisis de riesgos.
- Seguimiento de incidentes, para futuros análisis de riesgos.
- Listado centralizado de los servicios y administradores de la institución.
- Políticas de uso de red para la institución, que respaldan y apoyan los controles implementados, con un diseño que permite su fácil actualización y control de cambios.
- Documentación completa de la topología de la red.
- Memorias Técnicas de los equipos de telecomunicaciones.
- Respaldos de la configuración actual de los equipos de telecomunicaciones.
- Procedimientos de respaldos de los equipos de telecomunicaciones.
- Configuración de manera segura en los equipos de telecomunicaciones.
- Procedimientos de configuración de servidores, servicios y equipos activos.
- Acceso sólo a servicios necesarios para administradores y usuarios, cuando se intenta acceder a los recursos del segmento, por medio del firewall implementado y hardening en servidores.
- Bitácoras de acceso no autorizado en el perímetro de red.
- Análisis de tráfico en tiempo real.
- Permitir a los usuarios internos sólo acceso a servicios válidos, limitando la posibilidad de que un ataque se lleve desde la organización.
- Reducir el ancho de banda generado por malware desde el interior de la organización, intencional o no, que pueda afectar a otras redes.

- Bitácoras del tráfico que pasa por el perímetro de red.
- Contemplando los puertos válidos por el firewall, apoya la tarea de monitoreo un IDS sobre los servicios permitidos hacia la institución y sus ataques conocidos a éstos, permitiendo tomar medidas sobre dichos comportamiento.
- Creación de reglas específicas que permitan detectar algún tipo de tráfico en particular.
- Gráficas de ancho de banda utilizado por protocolo.
- Gráficas de ancho de banda utilizado por servicio.
- Gráficas de ancho de banda utilizado por host.
- Gráficas de uso de ancho de banda, por parte del proveedor de servicios DGTIC y su mesa de ayuda "www.noc.unam.mx".
- Contribuir a evitar el uso indebido de ancho de banda por medio de gestores de contenido.
- Adecuar el contenido no deseado de internet de acuerdo con las políticas de uso válido.
- Reducir riesgos legales por la descarga y compartir software.
- Informes de los 100 sitios más solicitados donde se emplee filtrado de contenido.
- Informes de los 100 sitios menos solicitados donde se emplee filtrado de contenido.
- Políticas de filtrado web que permitan emplear los recursos de una manera productiva y positiva.
- Reportes de uso de la red inalámbrica.
- Monitoreo de uso de la red inalámbrica por día, cuenta de usuario o MAC address.
- Capacidad para la elaboración de manera periódica de informes.
- Soporte en hardware y respaldo eléctrico para nuevos servicios.
- Aumento en la capacidad de almacenamiento de respaldos.

Para garantizar la seguridad de la información dentro de la institución, no sólo se requiere de la implementación de los diferentes mecanismos de control, ya que no serán suficientes si no se cuenta con el personal adecuado que garantice su operación. Como responsables de seguridad siempre debemos considerar la capacitación constante, que nos permita responder a futuros incidentes.

Cuando se busca establecer un esquema de seguridad, uno de los principales problemas es la forma de trabajo y el desinterés por temas relacionados con la seguridad, para la mayoría de los usuarios, los temas de seguridad de la información representan limitantes para el desarrollo de sus actividades o incluso molestias. Remarcar la importancia de la seguridad de la información para usuarios finales es una de las tareas que la Secretaría de Informática tiene que reforzar, para transmitir la importancia que tiene la seguridad apoyada con las políticas establecidas que permita ver a la seguridad, no como una limitante que dificulte su trabajo, sino como procedimientos y mecanismos de apoyo, que auxilien el correcto desempeño de sus actividades.

En general, el proyecto se logró concluir de manera satisfactoria, se utilizaron los recursos existentes, la mayoría de los controles implementados no representaron costos significativos, lo que implicó un ahorro para la institución.

No podemos decir que los controles, procedimientos, políticas y recursos humanos empleados, garantizan el 100% de la seguridad de la institución, ya que como nos dimos cuenta, existen riesgos residuales, que por las características propias de cada institución no son atendidos de manera inmediata. El trabajo desarrollado permite llevar a la institución a un proceso de mejora continua, que ayude a responder de mejor manera ante un incidente.

A la fecha los planteles que integran el Colegio de Ciencias y Humanidades no cuentan con un esquema de seguridad, por lo que se encuentran expuestos en su totalidad, una meta a corto plazo es unir esfuerzos para lograr la implementación en los diferentes planteles, para que con ello se pueda llegar a desarrollar un esquema de seguridad de acuerdo con sus necesidades, razón por la cual se torna importante invertir en capacitación, tecnología y los recursos humanos necesarios.