INFRAESTRUCTURA DE COMUNICACIÓN DE DATOS PARA ADMINISTRAR LA INFORMACIÓN DE JUICIOS LABORALES EN MÉXICO

DATA COMMUNICATION INFRASTRUCTURE TO MANAGE LABOR LITIGATION INFORMATION IN MEXICO

Cruz Oswaldo del Toro Mejia
Docente en el Instituto Tecnológico de Colima, Colima (México).
E-mail: g1646002@itcolima.edu.mx ORCID: https://orcid.org/0000-0002-7407-3216

Juan Garcia Virgen
Docente en el Instituto Tecnológico de Colima, Colima (México).
E-mail: jgarcia@itcolima.edu.mx ORCID: https://orcid.org/0000-0002-8913-427X

Ramona Evelia Chávez Valdéz
Docente en el Instituto Tecnológico de Colima, Colima (México).
E-mail: echavez@itcolima.edu.mx ORCID: https://orcid.org/0000-0002-5697-6825

J. Reyes Benavides Delgado
Docente en el Instituto Tecnológico de Colima, Colima (México).
E-mail: rbenavides@itcolima.edu.mx ORCID: https://orcid.org/0000-0002-6190-5933

Recepción: 16/03/2018. **Aceptación:** 19/06/2018. **Publicación:** 28/09/2018

Citación sugerida:

Toro Mejia, C. O. del, García Virgen, Juan, Chávez Valdéz, R. E. y Benavides Delgado, J.R. (2018). Infraestructura de comunicación de datos para administrar la información de juicios laborales en México. *3C TIC. Cuadernos de desarrollo aplicados a las TIC*, 7(3), 40-57. doi:http://dx.doi.org/10.17993/3ctic.2018.61.40-57/

RESUMEN

En esta investigación se desarrolló un modelo de comunicación de datos que da seguimiento a los juicios laborales, protegiendo los datos personales, y permitiendo un mejor acceso a la información, aplicando la normativa internacional y leyes domésticas que rigen la seguridad de archivos digitales y datos personales. En el análisis del proceso, a través de entrevistas semiestructuradas se detectó la falta de articulación entre las unidades organizativas, provocando que la consulta de información y transcripción consuma jornadas completas del personal. Como solución, se creó un repositorio de información seguro que permita la disponibilidad y confidencialidad de la información a través de herramientas como Windows Server y Arreglos de Discos para asegurar la integridad de la información y recuperación de errores.

ABSTRACT

In this research, a data communication model was developed that tracks labor trials, protecting personal data, and allowing better access to information, applying international regulations and domestic laws that govern the security of digital files and personal data. In the analysis of the process, through semi-structured interviews, the lack of articulation between the organizational units was detected, causing that the consultation of information and transcription, consumes complete days of the personnel. As a solution, a secure information repository was created that allows the availability and confidentiality of information through tools such as Windows Server and Disk Arrays to ensure the integrity of information and recovery of errors.

PALABRAS CLAVE

TIC, E-justicia, Seguridad de la información, Protección de datos personales, Repositorio de datos.

KEY WORDS

ICT, E-justice, Information security, Personal data protection, Data warehouse.

1. INTRODUCCIÓN

En México, hasta el año 2017, los juicios laborales han sido arbitrados a través de las Juntas Locales de Conciliación y Arbitraje según rige la Ley Federal del Trabajo. Para el 2016 se anuncia "una reforma al artículo 123 constitucional y también cambios a la Ley Federal del Trabajo" (Amezcua Hornelas, 2016). Esto indica un cambio en el proceso de los juicios laborales, pasando la jurisdicción del poder ejecutivo al judicial, y la oportunidad ideal para realizar una investigación sobre la forma en que se administra la justicia laboral que, como definen Restrepo Pimienta y Caraballo Beleño (2015), para que esa administración de justicia pueda ser considerada acorde a las necesidades y exigencias que la sociedad requiere, tiene que estar revestida de unas características que le permitan colmar las expectativas que el conglomerado tiene respecto a la misma. Una de esas características... es la rapidez con la cual resuelva los conflictos que le son planteados.

La clave de esta definición es la rapidez, y para esto se ha realizado un estudio sobre las necesidades que los encargados de administrar los juicios laborales tienen que solventar para agilizar el proceso.

Mirando hacia fuera de México, encontramos significativas implementaciones para la mejora de procesos en e-justicia. Se tiene a Singapur como punta de lanza con la burocracia más efectiva del mundo (Hira, 2014). Por otro lado, el Reino Unido habría invertido al menos 390 millones de libras para dotar a los juzgados de un sistema de software para los casos de delincuencia menor (Sommerville, 2005). En EE.UU., podemos encontrar artículos sobre la utilización de bases de datos para generar estadísticas en el ámbito legal, como es el caso del artículo Machine-readable data files: Statistics on crime and criminal justice, donde se utilizaron fuentes de datos como CJAIN, NCJRS, destacando que la Red de Información y Archivo de Justicia Penal (CJAIN por sus siglas en inglés) fue fundada en 1978 para permitir el acceso compartido de la información (Rowe y Anderson, 1986).

En el estado del arte en sistemas de información para e-justicia se observa un estudio sobre las implementaciones de TICs en diferentes naciones. Como ya mencionamos, Singapur, pero se incluye a Brasil, Bélgica, Portugal y Cape Verde con la metodología que estudia las categorías de tecnología, organización y complejidad (Velicogna, 2007). Singapur, en 1991 lanzó el proyecto ATOMS que consistió en kioscos para pago de multas que tenían la característica de permitir a la ciudadanía poder declararse culpable para delitos de tipo civil. Para Brasil, en 2014 se diseñó un proyecto con requerimientos como: proveer de equipo de cómputo a todas las cortes y desarrollar un sistema que unificara el sistema de justicia (Rosa, *et al.*, 2013). Bélgica por su parte, tenía el problema de letargo y retraso en los juicios que llegaban a durar hasta nueve años, el primer paso fue equipar con

computadoras las cortes e incluso laptops para todos los jueces. Esto permitió una serie de intentos para desarrollar proyectos de ámbito local hasta llegar al ambicioso y fallido proyecto Phenix que buscaba ser implementado en todas las cortes, almacenar toda la información legal de cada caso sin importar que fuera mercantil, penal, administrativo, civil, etc. (Poullet, 2009). Sin embargo, durante la implementación notaron un problema, pues no se había previsto un esquema de recuperación de la información en caso de catástrofe hasta ya muy avanzado el proyecto, al punto de tomar la decisión de dejarlo en espera por no haber realizado el respectivo análisis de riesgos (Cerrillo y Fabra, 2009).

La seguridad de los datos personales es actividad cotidiana para muchos países, debido a la era digital y de telecomunicaciones, esto ha obligado a los administradores de justicia a implementar medidas para hacer cumplir la ley.

La seguridad de los datos personales es actividad cotidiana para muchos países, debido a la era digital y de telecomunicaciones, esto ha obligado a los administradores de justicia a implementar medidas para hacer cumplir la ley, como en Uruguay, donde se diseñó un sistema para anonimizar la documentación (Vico y Calegari, 2015). En México, por su parte, en el año 2010 se promulgó la ley de protección de datos que garantiza la privacidad y el derecho a la autodeterminación informativa de las personas (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010). Dicha ley rige el comportamiento y manejo de información para particulares pero no fue hasta 2017 cuando se promulgó la ley que rige a las unidades organizativas públicas o que reciban recursos públicos (Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017). El hecho de que hayan pasado siete años entre las diferentes publicaciones nos habla de la urgencia que tienen las entidades gubernamentales de implementar esquemas de seguridad en la información.

Durante el análisis documental, se detectaron que muchas implementaciones de TICs para temas de e-justicia han fracasado dado que fueron implementadas a gran escala y no se consideraron escenarios como recuperación de errores y evaluación de riesgos. La solución que se presenta consiste en la creación de un modelo unificado que permita a las juntas locales y/o juzgados, la posibilidad implementar una infraestructura de comunicación de datos con enfoque a la seguridad de la información, basada en estándares de calidad internacional, dicha infraestructura permite la escalabilidad de lo local a lo nacional.

Ed. 26. Vol.7 Nº 3. Septiembre-Diciembre 2018
DOI: http://dx.doi.org/10.17993/3ctic.2018.61.40-57/

2. METODOLOGÍA

Para el caso de estudio de la Junta Local de Conciliación y Arbitraje del Estado de Colima en México, después de haber hecho la investigación documental, se llevaron a cabo entrevistas semiestructuradas para la obtención de datos cualitativos con todos los involucrados en el proceso de los juicios laborales, de acuerdo a las recomendaciones y estructura propuesta por Hernández Sampieri, *et al.* (2010). La lista de entrevistados se obtuvo del organigrama general de la Junta Local de Conciliación y Arbitraje de Colima cuya organización en su representación más general podemos observar en la Figura 1.

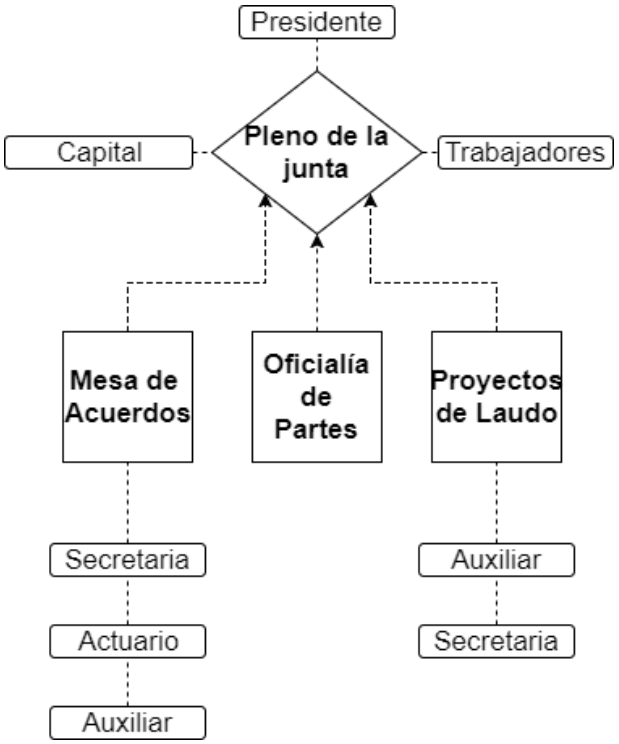

Figura 1. Diagrama organizacional de la Junta Local.

En la reforma a los artículos 107 y 123 de la Constitución Política Mexicana se establece la eliminación de las Juntas para ser sustituidas por un Tribunal, y así el Pleno sea reemplazado por un Juez, el resto de la estructura se mantiene similar de acuerdo con el decreto de reforma firmado por

el Poder Ejecutivo y Secretaría de Gobernación (2017).

Tras las sesiones de entrevistas, se continuó con la etapa de análisis y diseño a través de diagramas de secuencia, casos de uso y de flujo. En la Figura 2 podemos observar el diagrama de secuencia para un juicio o procedimiento ordinario. Se determinó también durante éstas fases, el nivel de acceso a la información, es decir la autorización acorde al puesto se puede observar en la Figura 3.

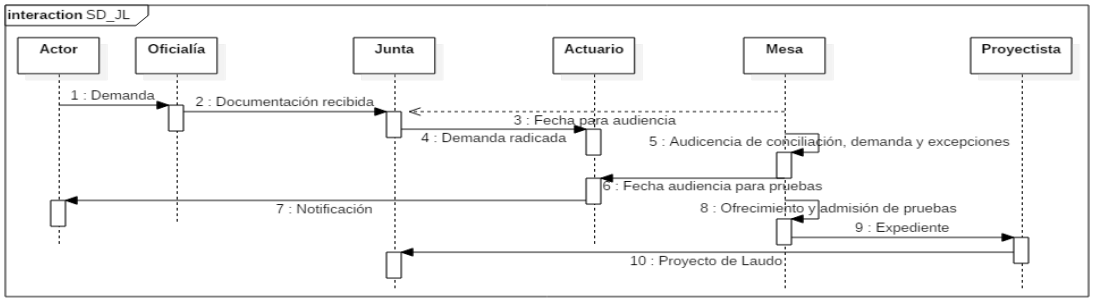

Figura 2. Diagrama de secuencia de un Juicio Ordinario.

Figura 3. Autorización para leer información.

La infraestructura de comunicación de datos deberá gestionar los riesgos cumpliendo con la metodología de las cinco metas tradicionales (Cárdenas-Solano *et al.*, 2016):

1. Seguridad adecuada a disponibilidad
2. Confidencialidad
3. Integridad o recuperación de errores
4. Control de accesos
5. Auditoría

Para cumplir con las primeras dos metas se ha diseñado un esquema de red, con servidores que administran un directorio activo a través de un controlador de dominio. Este se encarga de autenticar a los usuarios en su propio equipo de cómputo y garantizar la integridad de la información, haciendo uso de herramientas que permitan la recuperación de la información aun cuando los sistemas de almacenamiento y respaldo fallen. Para mitigar el riesgo se utilizan los arreglos de discos en una Storage Area Network (Naden, 2015) que permiten perder hasta dos unidades físicas sin perder información. Por último, las metas de control de accesos y auditoría están a cargo de las herramientas de Windows Server©. Las cinco metas buscan el cumplimiento de estándares internacionales aplicables a organizaciones que almacenan información legal como evidencias y expedientes legales como es el caso de estudio que se presenta (Lazarte, 2012).

3. RESULTADOS

Atendiendo las metas mencionadas en el artículo de Cárdenas-Solano, *et al.*, (2016), se diseñó un modelo que presenta una red de computadoras y dispositivos periféricos, como se muestra en la Figura 4. La red como parte de la propuesta de solución considera un *site*, que incluye un servidor con la respectiva configuraron física y lógica, adicionalmente se diseñó una base de datos intrínsecamente segura, la base de datos será consumida a través de una aplicación web desarrollada por un equipo de programadores ajenos al caso de estudio y estará administrada por la seguridad del servidor. Este modelo tiene la finalidad de entregar al organismo público, una infraestructura de comunicación de datos que atiende el correcto seguimiento y administración de los juicios laborales con seguridad apegada a los estándares internacionales.

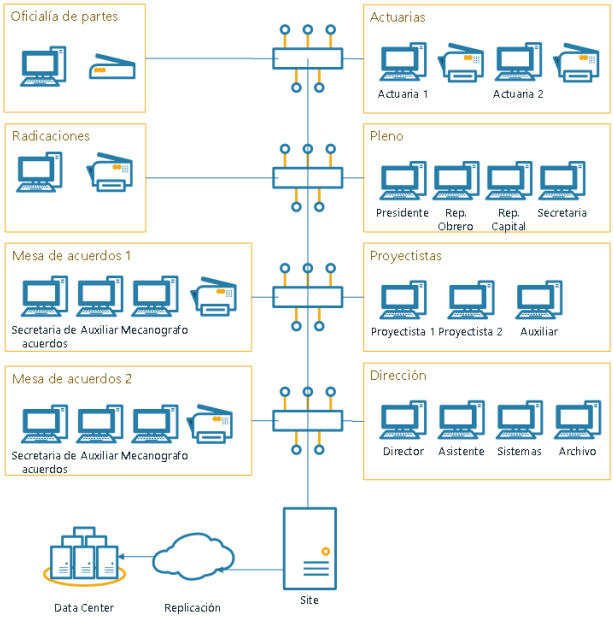

Figura 4. Esquema de red.

El *site* es el corazón de la comunicación de datos y debe contener los equipos e infraestructura necesaria para la administración y seguridad de la información. Cada organización puede agregar o quitar elementos de acuerdo a las necesidades, el diagrama propuesto en la Figura 5 corresponde al equipamiento estándar y cableado necesario para el desarrollo de las actividades, que no se considera una red inalámbrica por ser menos seguras al estar más tiempo expuestas (Goodin, 2017).

DOI: http://dx.doi.org/10.17993/3ctic.2018.61.40-57/

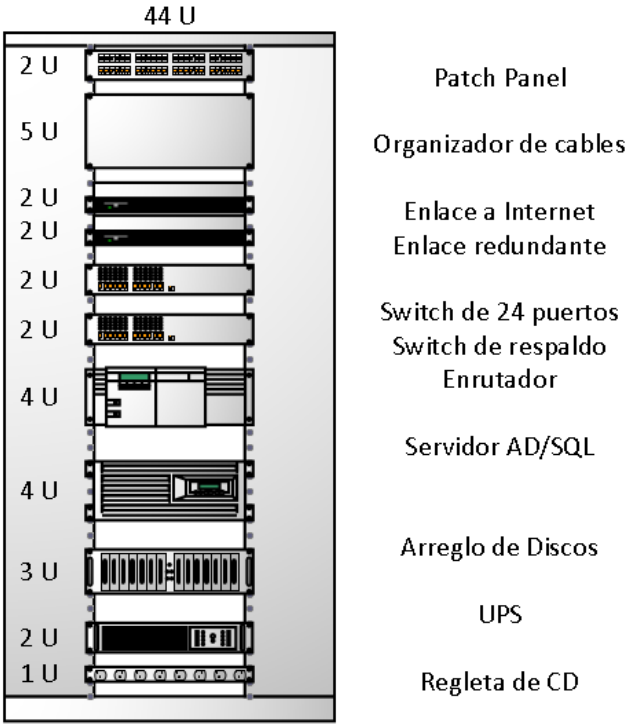

Figura 5. Rack para el Site.

El *patch panel* es la pieza donde terminan todos los cables que se distribuyen por el edificio utilizando la norma T568B, conocida internacionalmente para cableado estructurado por su facilidad de instalación y mantenimiento (Harrington, 2007). El siguiente elemento es el organizador de cables (*Patchlink*), que consiste en una pieza de polímero que permite la correcta organización del cableado que va a llegar al panel de parcheo. Una de sus principales funciones es que permite trabajar los cables del panel sin correr el riesgo de que se jalen y se suelten de éste, de manera que agrega una protección física.

La programación del *switch* consiste simplemente en activar y desactivar puertos según sus condiciones de uso, así si un equipo llega a la red no tendrá conexión física sino hasta que le activen el servicio por parte del administrador.

De los elementos más importantes, junto al servidor, es el arreglo de discos (SAN). Existen diversos arreglos estándares, para la implementación de la solución se necesitan por lo menos 6 unidades de discos duros de 1 TB en un arreglo RAID 6, que permita contar con un almacenamiento total de 2 TB para almacenamiento de información (en espejo) y 2 TB para paridad esto da la posibilidad de perder y sustituir hasta dos discos sin perder información.

Servidor AD

El controlador de dominio es un rol de *Windows Server Active Directory* (AD), y permite crear los elementos que conforman la red (dominio) y así regirse por las reglas establecidas en los *Group Policy* (GPO) o conocidas también como Directivas de Grupo. Dichas directivas determinan los permisos tanto del usuario como del equipo (Tankard, 2012). Por ejemplo, se puede restringir si el usuario tiene permiso de copiar a USB, instalar una impresora, modificar los parámetros de red, etc.

Las directivas disponibles son miles y pueden variar de acuerdo a las necesidades de cada implementación, pero para este caso de estudio, se deben asignar por lo menos las directivas que se muestran en la Tabla 1 a los usuarios del dominio:

Tabla 1. Directivas de Grupo (GPO).

Directiva	Rol
Cambiar Zona horaria	Administrador
Cambiar Hora del sistema	Administrador
Instalar Drivers	Administrador
Denegar inicio de sesión remoto	Todos
Hacer copias de seguridad	Sistema
Mensaje legal de bienvenida al dominio	Todos
Permitir apagar el equipo sin iniciar sesión	Todos
Requerir elevar privilegios para ejecutables	Usuarios del dominio
Bloquear Cuentas de inicio de sesión de Microsoft	Todos
Instalar impresoras	Administrador
Ejecutar desde CD-ROM- Memoria Flash	Administrador
Límite de inactividad del equipo	600 segundos
Número de inicios de sesión almacenados en cache (si DC no está disponible)	10
Requerir contraseña segura	Mayúsculas y caracter especial.
La contraseña expira tras	45 días
Unidades de almacenamiento externo	Sólo lectura, no ejecución
Permitir uso de Cortana	No

DOI: http://dx.doi.org/10.17993/3ctic.2018.61.40-57/

Directiva	Rol
Permitir indexación de archivos	Si
Restringir la instalación de programas no firmados.	Usuarios del dominio
Modificar los parámetros de Red (IP, DNS)	Administrador
Permiso de escritura a CD-ROM/Memoria Flash	Administrador
Permiso de lectura a CD-ROM/Memoria Flash	Oficialía, Mesa, Pleno.

Para el correcto funcionamiento del controlador de dominio, todos los equipos de cómputo deberán tener configurado como DNS la IP local del servidor, de manera que puedan ser respondidas las peticiones (Hannifin *et al.*, 2010).

Servidor SQL

Una vez establecidas las reglas de acceso a la red y creado el cerco de seguridad, se puede operar de manera segura un sistema de información, ya que el sistema de archivos por sí solo no es suficiente para la generación de reportes e información relacional, pues además de los archivos y documentos se requiere capturar determinada información de manera que se pueda obtener relaciones y hacer consultas para generar reportes. Para el modelo se utiliza SQL *server*, dado que permite usar la autenticación de Windows del dominio como método de autenticación para el servidor de base de datos y autorización de acceso a la información (Siegel *et al.*, 1994).

En la Figura 6 podemos observar el diagrama ER, que permite mantener la integridad de la información y la consulta. Los prefijos en los nombres de los campos, permiten una codificación más rápida de las consultas además evita que se adivinen los campos utilizando inyección SQL.

Una vez establecidas las reglas de acceso a la red y creado el cerco de seguridad, se puede operar de manera segura un sistema de información, ya que el sistema de archivos por sí solo no es suficiente para la generación de reportes e información relacional.

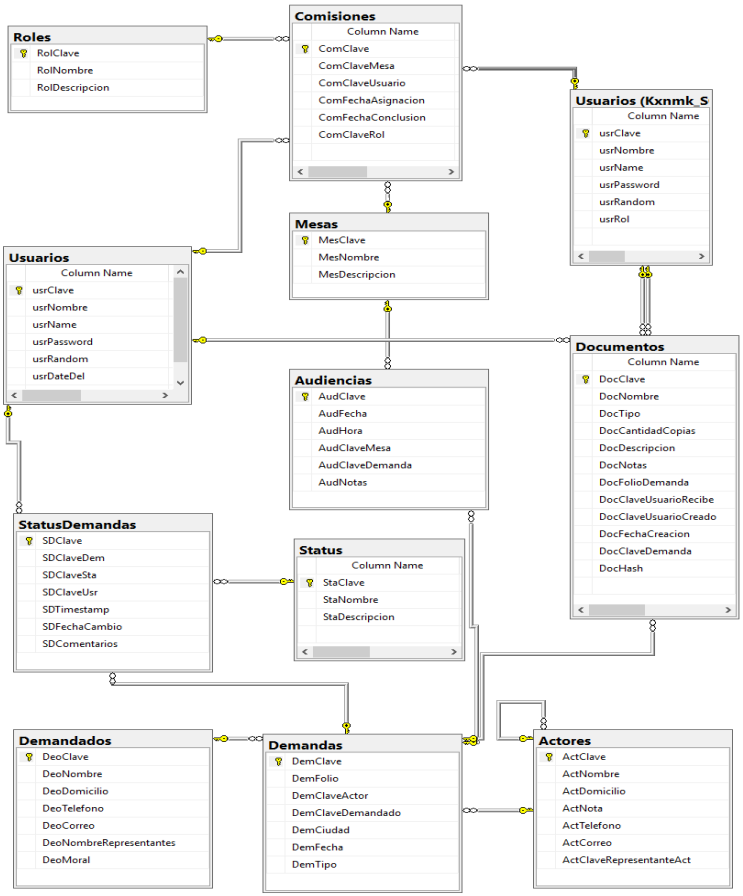

Figura 6. Diagrama base de datos.

Reducción de riesgos

Finalmente, con la utilización de las herramientas descritas podemos conocer los riesgos y establecer las estrategias que se implementan para mitigarlo. En la Tabla 2 se observa una lista con los posibles riesgos y se indica cuál es la herramienta que se utiliza como solución. Los riesgos mayormente consisten en agujeros de seguridad física y lógica, así como en personal que busca obtener o filtrar información, sin embargo, también se consideran los riesgos del desgaste común de los equipos mecánicos.

Tabla 2. Relación de riesgos de seguridad.

Riesgo	Protocolo de Solución
Se infiltra un equipo a la red del organismo.	La red local tiene deshabilitados los puertos y solo pueden ser activados en el switch por el administrador.
Se trata de infiltrar un equipo a la red del organismo por wifi.	La red cableada estará independiente de la red inalámbrica, si es que se decide implementar una red inalámbrica.
Se intenta ingresar a la red del organismo usando un equipo dentro de la red.	El servicio de autenticación de Window Server le requerirá usuario y contraseña dentro de las horas laborales del organismo.
Se intenta adivinar o usar fuerza bruta sobre la contraseña para obtener acceso a los recursos de la red.	El servidor bloqueará la cuenta al tercer intento y sólo podrá ser utilizada hasta que el administrador la libere.
Se obtiene un usuario y contraseña de un miembro de la organización.	El sistema le permitirá acceder sólo a los archivos a los que tiene permiso dicha cuenta.
Se accede a los recursos de la red para robar información.	El equipo no permite el almacenamiento en dispositivos externos.
El personal decide eliminar toda la información almacenada en el equipo.	Los respaldos almacenados en el servidor permiten recuperar información perdida en los equipos del organismo.
El organismo ha quedado sin suministro de energía eléctrica	El UPS y no-breaks permiten apagar de forma segura los equipos y servidores de manera que no se pierda información
Uno de los discos duros donde se almacena la información del organismo se ha dañado.	La SAN configurada con RAID 6 permite perder y reemplazar hasta dos discos duros sin perder información.
Un disco duro de los equipos de la organización se ha dañado.	La serie de respaldos almacenados en el servidor permitirán recuperar la información una vez reemplazado el disco. La configuración del arreglo de discos permite perder hasta dos discos.

4. CONCLUSIONES

Cuando se analizan proyectos de TICs, es común pensar en un sistema de información que facilite la administración de la información, sin embargo, es necesario determinar el riesgo técnico y jurídico de comprometer la información, en especial hablando de datos legales y de carácter personal. Por lo tanto, el primer paso en la implementación de TICs deberá ser el análisis de la seguridad y se deben cuidar todos los ángulos.

Con la infraestructura e implementación correcta de la comunicación de datos, mitigamos los riesgos que van desde pérdida o corrupción de la información hasta filtraciones. Al impedir que los equipos puedan escribir en unidades de almacenamiento externo o enviar a impresoras no oficiales, se reduce la posibilidad de filtraciones y restringir el acceso al sistema de información sólo desde la red local reducimos el riesgo de *malware*. Se asegura la información de manera física con un arreglo

de discos que nos permite reemplazar hasta dos unidades de almacenamiento dañadas. Se restringe también la posibilidad de instalar y ejecutar aplicaciones, reduciendo así las posibilidades de ser infectados por *malware*, cumpliendo así las cinco metas tradicionales en la gestión de riesgos.

> Con la infraestructura e implementación correcta de la comunicación de datos, mitigamos los riesgos que van desde pérdida o corrupción de la información hasta filtraciones.

El modelo también permite la creación y administración de una base de datos por un sistema gestor que controla el acceso, es decir usando la misma autenticación de Windows, se determina el nivel de acceso a la información dentro de la base de datos y por supuesto, facilita la elaboración de consultas y reportes que pueden ser consumidos desde una página web.

La solución abre paso a la implementación de TICs para la administración de los juicios laborales, sin embargo, no está todo hecho, pues la minería de datos y generación de datos estadísticos, ayudarán en el proceso de mejorar la toma de decisiones, permitiendo llegar a una sociedad más justa e instituciones con una mejor experiencia de usuario.

5. REFERENCIAS BIBLIOGRÁFICAS

Amezcua, N. (2016). *Juntas locales y federales de conciliación y arbitraje desaparecerán*. Recuperado el 11 de Septiembre de 2017 de: http://www.frecuencialaboral.com/juntasdeconciliaciondesapareceran2016.html

Cárdenas-Solano, L., Martínez-Ardila, H., y Becerra-Ardila, L. (2016). Gestión de seguridad de la información: revisión bibliográfica. *El Profesional de La Información*, 25(6), pp. 931–948. doi:https://doi.org/10.3145/epi.2016.nov.10

Cerrillo, A., y Fabra, P. (2009). *E-Justice: Information and Communication Technologies in the Court System.* IGI Global.

Hannifin, D., Alpern, N., y Alpern, J. (2010). Chapter 10 - Securing Windows Server 2008 {R2}. En: *Microsoft Windows Server 2008 {R2}* (pp. 461–532). Nueva York, EE.UU.: Syngress. doi:http://dx.doi.org/10.1016/B978-1-59749-578-3.00010-4

Harrington, J. (2007). 3 - Fast and Gigabit Ethernet Media and Standards. En *Ethernet Networking for the Small Office and Professional Home Office* (pp. 41–54). EEUU: Morgan Kaufmann Publishers. doi:http://dx.doi.org/10.1016/B978-012373744-1/50029-2

Hernández, R., Fernández, C. y Baptista, M. (2010). Metodología de la Investigación (Quinta). Nueva York, EE.UU.: McGrawHill.

Hira, A. (2014). Building a more efficacious Chilean bureaucracy: lessons from the Singapore case. *Revista de Gestión Pública*, 3(2), pp. 279–296.

Lazarte, M. (2012). *Guilty or not? New ISO/IEC standard for credible digital evidence.* Recuperado el 25 Septiembre, 2017, de: https://www.iso.org/news/2012/11/Ref1677.html

México, Cámara De Diputados Del H. Congreso de la Unión. (2017). *Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados*, Diario Oficial de la Federación. Recuperado el 12 de Septiembre, 2017 de: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

México, Cámara De Diputados Del H. Congreso de la Unión. (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Diario Oficial de la Federación. Extraido el 12 de Septiembre, 2017 de: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

México, Poder Ejecutivo y Secretaría de Gobernación. (2017). Decreto por el que se declaran reformadas y adicionadas diversas disposiciones de los artículos 107 y 123 de la Constitución Política de los Estados Unidos Mexicanos, en materia de Justicia Laboral. Recuperado el 24 de Noviembre, 2017 de: https://www.gob.mx/cms/uploads/attachment/file/234847/Decreto_DOF_Reforma_CPEUM_24.02.17.pdf

Naden, C. (2016). *Taking information security management to another level with a new standard for specific market sectors*. Recuperado el 25 de Septiembre, 2017 de: https://www.iso.org/news/2016/08/Ref2107.html

Naden, C. (2015). *Keeping data safe - what's your back up?* Recuperado el 25 de Septiembre, 2017 de: https://www.iso.org/news/2015/01/Ref1926.html

Poullet, Y. (2008) The Belgian Case: Phenix or How to Design E-Justice Through Privacy Requirements and in Full Respect of the Separation of Powers? En Cerrillo, A., Fabra, P. (Eds.), *E-Justice: Information and Communication Technologies in the Court System* (pp. 186-195). New York, EE.UU.: InformatIon Science Reference. doi:https://doi.org/10.4018/978-1-59904-998-4.ch012

Restrepo, J., y Caraballo, R. (2015). Procedimiento ordinario laboral en Colombia y Venezuela análisis comparativo. *Advocatus*, 12(24), pp. 173–186.

Rosa, J., Teixeira, C., y Sousa, J. (2013). Risk factors in e-justice information systems. *Government Information Quarterly*, 30(3), pp. 241–256. doi:https://doi.org/10.1016/j.giq.2013.02.002

Rowe, J., y Anderson, S. (1986). Machine-readable data files: Statistics on crime and criminal justice. Government Publications Review, 13(2), 243–247. doi:https://doi.org/10.1016/0277-9390(86)90007-5

Siegel, M., Madnick, S., y Sciore, E. (1994). Context interchange in a client-server architecture. *The Journal of Systems and Software*, 27(3), pp. 223–232. doi:https://doi.org/10.1016/0164-1212(94)90044-2

Sommerville, I. (2005). Ingeniería del Software. En Miguel Martín-Romo (Ed.), 2005 (7a ed., p. 550). Madrid, España: Pearson Addison-Wesley.

Tankard, C. (2012). Taking the management pain out of Active Directory. *Network Security*, (4), pp. 8–11. doi:https://doi.org/10.1016/S1353-4858(12)70025-9

Velicogna, M. (2007). Justice systems and ICT What can be learned from Europe? *Utrecht Law Review*, 3(1), pp. 129–147. doi:https://doi.org/10.18352/ulr.41

Vico, H., y Calegari, D. (2015). Software architecture for document anonymization. *Electronic Notes in Theoretical Computer* Science, 314, pp. 83–100. doi:https://doi.org/10.1016/j.entcs.2015.05.006