La seguridad de los datos en las universidades públicas: entre la realidad y los desafíos

Yuhly del Carmen García
UNESR - Núcleo Caracas | *oficinadelegadacc@gmail.com*
Fecha de recepción: **15 mayo 2024**
Fecha de aceptación: **2 agosto 2024**[1]

Resumen

Este artículo explora la situación actual de la seguridad de los datos en las universidades públicas tomando mi experiencia personal y profesional vivida en un núcleo de la UNESR. Muestro como a pesar de las limitaciones presupuestarias, se ha logrado avanzar en la digitalización y sistematización de datos académicos y administrativos, así como en la creación de nuevas alternativas para digitalizar y sistematizar datos en la Oficina Delegada de Control de Estudios del núcleo donde laboro. Sin embargo, advierto sobre la necesidad de implementar nuevos protocolos para mejorar la seguridad de los datos y la información. Analiza situaciones reales que han surgido en los últimos años de pandemia por COVID-19 y postpandemia, evidenciando la necesidad de nuevos planes y estrategias para mejorar la seguridad informática y asumir la seguridad de los datos como una prioridad ahora que hemos avanzado en la transformación digital.

Palabras clave: Seguridad de los datos. Universidades públicas. Digitalización. Experiencia personal y profesional.

1 Soy venezolana, trabajadora universitaria con experiencia en el área de Control de Estudios. Licenciada en Pedagogías Alternativas, mención: Gestión Universitaria Digital. Jefa de la Oficina Delegada de Control de Estudios del Núcleo Regional de Postgrado y Educación Avanzada Caracas de la UNESR. Actualmente realizando estudios de Maestría en Gestión para la Creación Intelectual en la modalidad de estudios abiertos.

Introducción

Las universidades públicas, incluyendo la UNESR Núcleo Regional de Postgrado y Educación Avanzada Caracas, también conocido como Núcleo Postgrado Caracas, manejan una gran cantidad de datos sensibles, como información personal de estudiantes y profesores/as (en nuestro caso, por ser la única universidad de carácter andragógico del país, denominamos participantes y facilitadores/as), personal administrativo y obrero, además de datos financieros, información de investigaciones y de propiedad intelectual. Y, la seguridad de estos datos es crucial para proteger la privacidad de las personas, la integridad de las investigaciones y el buen funcionamiento de la universidad.

Pero también, las organizaciones universitarias públicas venezolanas se enfrentan hoy día a un desafío creciente, tal como nos lo recuerda Norjhira Romero Pérez, 2024; ello en la relación con la necesidad de generar ingresos propios para garantizar su sostenibilidad financiera. Este desafío se ha visto agravado por una serie de acontecimientos, tales como la disminución de los fondos públicos y las fluctuaciones económicas.

Si bien es cierto, antes del 13 de marzo de 2020, el Núcleo Postgrado Caracas tenía el sistema de Control de Estudios en intranet y un servidor local, no se contemplaba el trabajo 100% a distancia y no teníamos en nuestro radar laboral el hecho de trabajar 100% a distancia. Sin embargo, por razones de fuerza mayor y motivado a un virus invisible, además de mortal. A partir de ese mencionado día, todo cambió. La pandemia de COVID-19 obligó a la universidad a realizar un cambio radical, que nos condujo al trabajo 100% a distancia y surgieron nuevos

desafíos para la seguridad de los datos y la información.

Sin embargo, en nuestro caso, teníamos que empezar desde "otro principio", es decir, crear los mecanismos para obtener los datos y recopilar la información que sí teníamos completa en sede física (mediante planillas impresas que cada participante o nuevo ingreso entregó hasta ese mediodía del 13 de marzo de 2020), pero que por el confinamiento como medida necesaria para resguardar la salud y evitar la propagación, no podíamos desplazarnos a buscar.

Es así como junto a la profesora Norjhira (Coordinadora de la Maestría en Ciencias Administrativas mención Gerencia Pública, hoy en día; Directora del Núcleo Postgrado Caracas) empezamos a crear y utilizar los formularios en línea de *Google*, cuyo enlace compartimos en redes sociales y grupos de WhatsApp, pidiendo que lo hicieran llegar a más personas. Desde esos datos recogidos en dichos formularios, empecé a crear las listas de clases de ese nuevo período académico que iniciaba el 16 de marzo de 2020. Comenzamos a trabajar organizadamente en la nube con carpetas y archivos, lo cual generó una gran cantidad de enlaces que luego se organizó en Linktree (árbol de enlaces) ligero y sencillo desde cualquier dispositivo y navegador web.

La seguridad de los datos y la información en las universidades públicas

Hoy día, es justo y necesario que también nos ocupemos de la seguridad de los datos, como tema crítico para las organizaciones públicas que ya dieron el salto hacia su transformación digital. Toda vez que, implementando las medidas adecuadas, las universidades pueden proteger la privacidad de las personas, la integridad de las investigaciones

y el buen funcionamiento de la institución. Aunado al hecho jurídico, además que las universidades públicas están obligadas a cumplir con la Constitución de la República Bolivariana de Venezuela, en sus artículos 28, 58 y 61, los cuales establecen un marco y un mandato claro para desarrollar la regulación en materia de protección de datos personales y garantía de los derechos digitales.

Los principales riesgos que puede tener una universidad si no tiene seguridad en sus datos lo podemos mencionar como sigue:

La falta de conciencia, conocimiento y capacitación de usuarios (participantes, facilitadores, personal administrativo y autoridades), sobre, cómo proteger adecuadamente la información y evitar incrementar la vulnerabilidad.

La falta de un plan de continuidad operativa puede comprometer la disponibilidad de la información.

La información es un activo valioso que se puede crear, modificar o eliminar en una universidad, si se gestiona adecuadamente, le permite trabajar con confianza, pero para que esto se logre existe lo que se llama la seguridad de la Información. Según la ISO/IEC (2016), citado por E, Vega (2021):

> La seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada. Esta definición básicamente significa que debemos proteger nuestros datos y nuestros

> recursos de infraestructura tecnológica de aquellos quiénes intentarían hacer un mal uso de ellos. (Vega 2021; p. 20).

Desde que se logró digitalizar la información relacionada con la "Oficina Delegada de Control de Estudios", y ser canalizada por medio de la miniweb del Núcleo, siguiendo patrones de acceso con medidas básicas de seguridad y de manejo de información, que alimenta nuestra página informática, se ha logrado por medio de la constancia, dedicación y mística de trabajo, investigar cada una de las herramientas gratuitas de Google. Tomar las responsabilidades de manejar un área tan compleja como es Control de Estudios. No fue, ni es una tarea fácil porque son muchos los procesos que se deben cuidar, y más aún, si la mayoría de la información que se pública está en la nube, específicamente, en un Drive de Google, que cualquier dato si no se tiene una metodología de trabajo puede desaparecer con un solo clic.

Aunque estas herramientas gratuitas nos han ayudado al manejo de la información son vulnerables a diversas amenazas, podemos tener riesgo de acceso no autorizado y robo de datos confidenciales, la falta de controles de seguridad puede facilitar que accedan a información sensible.

Cuando en julio de 2023 facilité dos curso-talleres de 16 horas académicas sobre "Gestión/Autogestión Digital de Procesos y Procedimientos Administrativos de Control de Estudios desde la Miniweb del Núcleo". Uno dirigido al personal de Control de Estudios, y otro para Coordinadores(as) de Postgrado y Facilitadores(as), fue también para crear conciencia, en las y los usuarios, sobre la seguridad de los datos y la información, porque es una preocupación que tengo en la

gestión universitaria digital.

De allí, lo fundamental de implementar un programa de concienciación de seguridad informática que capacite a los usuarios sobre las posibles amenazas y la importancia de proteger los datos. Algunas estrategias efectivas incluyen desde la concientización, hasta las herramientas que se van a utilizar, la primordial de ellas, Formación y Conciencia: capacitar al personal y a los estudiantes en buenas prácticas de seguridad informática para reducir riesgos en el manejo de la información.

Estas prácticas contribuyen a preservar la confidencialidad, integridad y disponibilidad de la información en una organización, fortaleciendo su postura frente a posibles amenazas y garantizando un entorno seguro para los datos sensibles. Algo muy importante que ha consolidado el manejo de la Miniweb es que, en el Departamento de Control de Estudios todo el personal maneja la misma información, mientras todos manejan los mismos procesos, esto nos da como ventaja control, eficiencia y sobre todo seguridad.

Marco legal sobre la seguridad de los datos e información

Si bien Venezuela no posee una Ley específica de protección de datos personales, existen diversas normas que regulan la seguridad de la información y datos en diferentes ámbitos. A continuación, un resumen de las principales, contempladas como artículos en la Constitución, en la Ley orgánica de Telecomunicaciones y en otras similares que a continuación se enuncian:

Constitución de la República Bolivariana de Venezuela (CRBV, 1999):

» Artículo 28: Derecho a la información veraz, oportuna e imparcial.

» Artículo 60: Derecho a la protección del honor, vida privada, intimidad, propia imagen, confidencialidad y reputación.

Ley Orgánica de Telecomunicaciones (2000):

» Artículo 10: Protección de la privacidad de las comunicaciones.

» Artículo 11: Deber de los operadores de telecomunicaciones de garantizar la confidencialidad de la información de sus usuarios.

Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001):

» Establece el marco legal para las transacciones electrónicas.

» Regula la firma electrónica y los mensajes de datos.

Ley Especial Contra los Delitos Informáticos (2001):

» Tipifica delitos como el acceso ilícito a sistemas informáticos, la interceptación de datos y el sabotaje informático.

Decreto con Rango, Valor y Fuerza de Ley de Infogobierno (2014):

» Regula el uso de las tecnologías de información por parte del Estado.

» Establece principios para la protección de la información pública.

Reglamento de la Ley Sobre Mensajes de Datos y Firmas Electrónicas (2002):

» Desarrolla los principios y normas de la Ley.

» Establece los requisitos para la prestación de servicios de certificación de firmas electrónicas.

Normas COVENIN:

» Conjunto de normas técnicas venezolanas que establecen requisitos para la gestión de la seguridad de la información.

Es importante destacar que, a pesar de la existencia de todos estos articulados en estas leyes, reglamentos y normas, aún hace falta una Ley integral de protección de datos personales en Venezuela. No obstante, mientras eso llega también es importante tomar conciencia y actuar en beneficio de la seguridad de los datos y la información en las universidades públicas y en especial en la Oficina de Control de Estudios en el marco del desarrollo de las tecnologías en general y en especial de la inteligencia artificial, siendo esta última, aún incipiente. Por lo que se requieren nuevas leyes y regulaciones para garantizar el desarrollo responsable de la inteligencia artificial y proteger

los derechos de las personas.

La tecnología en las organizaciones universitarias públicas

La tecnología juega un papel fundamental en las organizaciones universitarias públicas, tanto en el ámbito académico como administrativo y en especial los asuntos relacionados con Control de Estudios. La tecnología puede ayudar a mejorar la calidad, accesibilidad y la eficiencia de la gestión digital.

Los avances en la tecnología han traído consigo un desafío a lo largo de su evolución, para quienes se dedican no solo a combatir el software malicioso, como los malware, troyanos, gusanos y virus que poseen diferentes clasificaciones dentro de la rama de la seguridad, sino que también existe una gran variedad de técnicas y métodos de ataques para vulnerar la era digital, por otro lado, los profesionales informáticos también se enfrentan a la obsolescencia debido a la falta de inversión de los recursos tecnológicos, en virtud a que sin una actualización, tanto de software como del hardware, no solo se pone en riesgo la información, sino que quedan expuestos a las vulnerabilidades que puedan explotar los delincuentes informáticos, en vista de que la proliferación de amenazas informáticas cada vez son más sofisticadas y poderosas.

Gestión digital y la miniweb del núcleo como ejemplo de buenas prácticas

Desde mi experiencia (analógica y digital) siendo jefa de la Oficina Delegada de Control Estudios del Núcleo Regional de Postgrado Caracas, considero que los datos son vitales para dicho departamento, pero también es importante la seguridad de la Información, la inversión en infraestructura, la capacitación del

personal, así como evaluar y seguir el impacto de la tecnología para asegurar que se esté utilizando de forma eficaz.

Cuando en marzo de 2020 llegó el confinamiento por la pandemia, caímos en cuenta que no teníamos la información debidamente organizada y resguardada, nos percatamos, que solo estaba de forma local (intranet), pero, sobre todo, no teníamos herramientas tecnológicas que nos permitieran acceder a ellas de forma remota. No obstante, algunas personas (docentes y personal administrativo) sin ser del área tecnológica, iniciamos la búsqueda de alternativas gratuitas que nos permitieran seguir las operaciones aún en cuarentena o confinamiento.

Pienso que, a veces, el personal no toma en serio la seguridad de la información, sino cuando se ve, en un atolladero, creemos que la información mejor guardada es la que está bajo candado en una computadora o la que maneja una sola persona. Por lo que me pregunto ¿qué ocurre si ese equipo se daña o la persona encargada de la información renuncia?, en esos casos, el departamento queda a la deriva, además porque muchas personas se creen dueña de la información y confunden el asunto público con lo privado-particular; asimismo porque que no conciben o saben trabajar en equipo, ni lograr un proceso sinérgico. Por ende, debemos concientizar al personal que labora en la universidad, en relación con este tema tan álgido y delicado, pero también de equiparnos con recursos tecnológicos para realizar el trabajo debido a que la información que se maneja es fundamental para la universidad. Entre ellas están: los expedientes de ingreso, egreso, notas, planillas de evaluación, entre otras, donde es primordial su información para que no sea corrompida o dañada.

No es ningún secreto para nadie, cuántos recursos

invierten algunas organizaciones para prevenir intrusiones manipulaciones que amenazan todo, desde la integridad de los datos; pero ¿qué ocurre con las universidades públicas que no poseen recursos económicos para ello? Para adquirir y sustentar sistemas que permitan la seguridad de la información, ya que las bases de datos de nuestros sistemas tienen información valiosa, tanto para nuestros participantes, facilitadores y personal administrativo.

Aquí es donde deben surgir las iniciativas para concientizar al personal, buscar herramientas que nos permita garantizar la protección de estos activos, así como se logró crear una miniweb en Linktree que es un sitio web gratuito que ofrece una especie de mini página personalizable. En dicha página se fueron insertando y reuniendo varios enlaces que redireccionan al usuario a los diferentes destinos (formularios en línea de inscripción, renovación y reporte de aranceles realizados con las herramientas gratuitas de gmail); así como canales de comunicación; repositorios de tesis, libros, buscadores; redes sociales, entre otros.

En dicha miniweb del Núcleo de Postgrado Caracas se busca, consulta y está disponible a través de internet las 24 horas del día y los 7 días de la semana, es una especie de oficina virtual con toda la información para gestionar en el Núcleo desde los procesos de ingreso, prosecución y egreso de los participantes, entre otros, con la validación y resguardo, accediendo de esa manera con cuentas de correo electrónico verificadas.

Sin embargo, estamos conscientes que los espacios gratuitos de almacenamiento en la nube pueden presentar algunos riesgos de seguridad que deben tenerse en cuenta, como las contraseñas de seguridad, las cuales deben ser

complejas y fácil de recordar para cada servicio de nube, y mantener una copia de seguridad de las credenciales de autenticación (password de recuperación) en caso de perderlas o no recordarlas. Aunque los proveedores de nube implementan fuertes medidas de seguridad, siempre existe el riesgo de que los datos puedan ser comprometidos, por parte de algunos usuarios, en virtud de que estos tienden a ser más vulnerables, no solo a aplicaciones engañosas y fraudulentas sino también a la manipulación física por parte de estos, o por programas que violen la seguridad de la propia nube, lamentablemente, las universidades han tenido que recurrir a estos espacios, por falta de presupuesto, es importante mantener copias de seguridad y/o respaldado en otros lugares como servidores o dispositivos de almacenamiento alternos para garantizar que la información quede completamente asegurada.

Hoy en día, las organizaciones dependen cada vez más de sus redes informáticas y un problema que las afecte, por pequeño que sea, puede poner en peligro la continuidad de sus procesos, provocando inevitablemente pérdidas de recursos, retrasos operativos y una crisis de confiabilidad en los datos, por eso surge la necesidad de crear planes de seguridad de la información. Donde se pueden implementar varias medidas para fortalecer la seguridad de la información en las universidades. No obstante, el tema más álgido sería no solo crear planes sino concientizar al personal en ese aspecto tan importante como lo es manejar la información y hacerles entender que no son dueños de esta última. Solo porque analizan la información, en mi experiencia he tenido que lidiar, con pocos recursos, tiempo limitado para dar respuesta, te conviertes en una herramienta para mejorar, así como plantea Norjhira Romero Pérez (2022) al señalar:

> Sin ser Gerente de Tecnología, operadora de Tecnología de la Información, ni graduada en el área, sí me convertí en estratega para la consecución de los objetivos básicos de la organización y por necesidad, aceleré el aprendizaje electrónico para garantizar el conocimiento de algunas plataformas tecnológicas avanzadas y de marketing para la dinámica de trabajo que imponía realidad en esta "nueva normalidad" signada por el confinamiento voluntario (p. 14).

Sin lugar a dudas, las organizaciones y su departamento de tecnología, en teoría, son los que deben encarar y realizar todo esto, pero hay casos como en el Núcleo, que no hay, o, es precisamente alguna o varias personas que no son del área tecnológica que buscan alternativas de soluciones e innovan en ese sentido.

Por ende, debemos visualizar alternativas desde nuestra experiencia, y la gran experiencia fue la pandemia por Covid-19, que nos enseñó, por medio de la tecnología que unido a las ganas de mejorar nuestro entorno laboral encontrásemos salidas exitosas en ese sentido. Es así como podemos lograr lo inimaginable, que es hoy en día, los recursos que tiene el Núcleo Regional de Postgrado Caracas en información. Además, un personal que trabaja día a día como hormigas (valga la metáfora) para que cada proceso no se detenga, y cuando hablo de recursos no es lo económico, sino las ganas de innovar utilizando quizás lo mínimo, pero sacándole provecho cada día a las herramientas gratuitas que podemos encontrar en las diferentes plataformas tecnológicas y redes.

Nuestra universidad no escapa de estos problemas como es tener datos corrompidos, información acéfala, y las áreas más

afectadas son las que mayor volumen de datos manejan, como lo son: las oficinas delegadas de control de estudios, el área de formación avanzada y por supuesto, el área de tecnología. Por qué se destacan estas tres áreas de funcionamiento, en específico. Por la sencilla razón de ser a nivel nacional las que se encuentran sin personal, sin un sistema de control de estudios, porque manejan la información de manera manual. Con el fenómeno de la partida del personal que dejó sus puestos de trabajo, por una razón u otra, de la misma forma se llevó buena parte de la información consigo.

Si bien los profesionales de la informática tienen una gran responsabilidad, no solo en configurar, aprender, investigar sobre nuevas tecnologías y proteger la información, también los usuarios tienen parte de esa responsabilidad en sus manos, ya que son ellos los que exponen sus propios datos y los de las organizaciones dejándola expuesta, tanto por el desconocimiento como la responsabilidad de seguir a cabalidad las medidas de seguridad. Por tal motivo es importante la formación continua de los usuarios para concientizar sobre la importancia de la Seguridad de la Información que manejan, en especial los sistemas que alimentan la data de las y los participantes que ingresan y egresan de nuestra institución, igual que los procesos que cada departamento ha realizado y las medidas necesarias para mantenerlos, así como la actualización de los datos más vulnerables, los cuales son las Bases de Datos de participantes (estudiantes).

Recomendaciones para mejorar la seguridad de los datos

Para mejorar la seguridad de los datos en las universidades públicas y en especial en la UNESR, recomiendo

tener presente que la gestión de datos en las universidades no se limita a resguardar la información. Es fundamental contar con herramientas que garanticen estabilidad, confiabilidad y seguridad en los datos que manejan los diferentes departamentos. En la actualidad, como ya fue planteado anteriormente, con frecuencia los usuarios u operadores que manejan información valiosa se retiran de las instituciones llevándose consigo dicha información, creyendo que les pertenece por haberla creado. Esto genera problemas en el desarrollo de las actividades de la universidad, ya que los departamentos pierden acceso a información crucial para la toma de decisiones, el seguimiento de procesos y la elaboración de informes.

1. Para fortalecer la seguridad lógica de la información en las universidades, se recomienda implementar una serie de medidas técnicas y administrativas, como las siguientes:

Medidas técnicas:

» Utilizar herramientas sencillas y fáciles de usar para los usuarios finales.

Bloqueo del equipo al ausentarse del mismo.

Prohibición de instalar herramientas sin autorización del departamento de informática.

» Implementar infraestructura de dominio con políticas de grupo (GPO).

Minimizar las posibles malas acciones de los usuarios.

Administrar las identidades de los usuarios.

Controlar los dispositivos USB y terminales en red.

» Mantener activo el *Firewall (sistema de seguridad de red)* a nivel del sistema operativo o del dispositivo de seguridad.

Proteger la red de accesos no autorizados.

» Proteger la información resguardada en discos o recursos compartidos.

Implementar soluciones especiales para detectar intrusiones.

Utilizar software antivirus y antimalware.

Medidas administrativas:

» Capacitar a los usuarios sobre la importancia de la seguridad informática.

Concientizarlos sobre las amenazas y las medidas que pueden tomar para protegerse.

» Establecer políticas de seguridad claras y concisas.

Definir los roles y responsabilidades de los usuarios

en materia de seguridad informática.

» Realizar auditorías de seguridad periódicas.

Identificar y corregir las vulnerabilidades en los sistemas informáticos de la universidad.

Beneficios de implementar estas medidas:

» Mejora en la seguridad de la información.

» Reducción del riesgo de ataques informáticos.

» Protección de los datos confidenciales de la universidad.

» Mayor confianza de los estudiantes, profesores y personal en la seguridad de la universidad.

La universidad está tomando medidas para garantizar la seguridad de los datos almacenando, copias de seguridad en diferentes lugares, como a través de un servicio basado en la nube que, según Redhat (2023) los servicios de nubes "son infraestructuras, plataformas o sistemas de software que los proveedores externos alojan y ponen a disposición de los usuarios a través de Internet". Esta elección puede generar ahorros de costos, una reducción de la carga de trabajo para el personal de TIC de la universidad y una rápida recuperación de información en caso de un problema.

Esto podría resolver uno de los puntos más resaltantes que algunos usuarios u operadores malintencionados, puedan adueñarse de la información, que, al ser despedidos, jubilados o decidan irse por el motivo que sea, se lleven información o los datos de la institución, logrando así crear fallas de seguridad y poca veracidad en la información. Esta situación es muy

importante ya que, debido al retiro de personal dentro de nuestra Universidad Simón Rodríguez, muchos departamentos han quedado sin información resaltante para la mejora y manejo de sus procesos, afectando la capacidad de respuesta.

Reflexiones finales

La seguridad de la información no es un mito, es una realidad, pero requiere inversión y compromiso. Existe una falsa creencia de que la seguridad de la información es sólo teoría. Sin embargo, la realidad es que es una necesidad vital en la era digital, donde la información es un activo invaluable. Destinar recursos en medidas de seguridad no es un gasto, sino una inversión que protege datos sensibles y evita daños económicos y reputacionales. Es cierto que algunas empresas de seguridad exageran las amenazas o incluso simulan ataques para vender sus productos. Elegir las herramientas adecuadas y aplicarlas correctamente es clave para proteger la información. Publicar información sensible sin las medidas de seguridad adecuadas es una grave negligencia. La información personal no es de dominio público.

La seguridad es un tema el cual no debe ser ignorado ya que actualmente en Venezuela no hay una Ley integral de protección de datos personales, es hora de tomar medidas para proteger los datos sensibles y garantizar la confianza de la comunidad universitaria. Es una responsabilidad compartida, es una necesidad real que requiere inversión, responsabilidad y compromiso por parte de todos para proteger la información personal y los activos informáticos.

Se ha intentado crear conciencia desde la creación de

la tecnología sobre la seguridad de los datos y los sistemas operativos. Nos han recordado por décadas utilizar contraseñas seguras y mantener bien resguardada nuestra información, pero hemos hecho caso omiso a los mensajes en ese sentido, la tecnología avanza y necesitamos ir a la vanguardia con ella y así lograr ser innovadores en las instituciones universitarias ya que son el pilar de las y los nuevos profesionales, de la sociedad y del país.

Como decía Steve Jobs *"La innovación no es cuestión de dinero, es cuestión de personas",* y cuya frase tiene mucho sentido para mí, porque significa que el éxito de la innovación no depende únicamente de la cantidad de recursos financieros disponibles, sino que también depende de las personas que participan en el proceso, dependen del talento, la creatividad, la capacidad y compromiso de las personas.

Referencias bibliográficas

Bucheli-Agam, S. (2018). La estructura organizacional en la gestión administrativa de las industrias del sector textil de la provincia de Tungurahua. Universidad Técnica de Ambato.

Constitución de la República Bolivariana de Venezuela. (1999, 30 de diciembre). Gaceta oficial de la República Bolivariana de Venezuela, No 36.860. [Extraordinaria], marzo 24, 2000.

Decreto con Rango, Valor y Fuerza de Ley de Infogobierno (2014) Publicada en Gaceta Oficial N. 40274.

Ley Especial contra los Delitos Informáticos (2001). Gaceta Oficial Nº 37.313 del 30 de octubre de 2001.

Ley sobre Mensajes de Datos y Firmas Electrónicas (2001). Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001.

Ley Orgánica de Telecomunicaciones Venezuela. (2000). Gaceta

Oficial N° 36.970 de la República Bolivariana de Venezuela. Caracas, 12 junio de 2000.

Normas Venezolanas COVENIN (2003). Gaceta Oficial N° 6.782 Extraordinaria 2003.

Red Hat (2023) ¿Qué son los servicios de nube?, https www.redhat.com.

Reglamento de la Ley Sobre mensajes de Datos y Firmas Electrónicas (2002). Decreto N. 3.335 de fecha 14 de diciembre de 2002.

Romero Pérez, Norjhira (2024). La nueva visión de la andragogía en las organizaciones universitarias públicas venezolanas en un contexto de asedio. Revista Educación y Ciencias Humanas. N° 50, 2024.

Romero Pérez, Norjhira (2022) Del Papel al Pdf y de éstos a la Transformación Digital Disruptiva en Tiempos de Pandemia por Sars-Cov2. Revista R- egresar. Año I N°1, enero-abril 2022.

Vega E (2021) Seguridad de la Información. Editorial Área de Innovación y Desarrollo, S.L.