Visión Antataura
Vol.8, No.1: 84-103
Junio – Noviembre, 2024
Panamá
ISSN L 2520-9892

Mecanismos de autentificación para el acceso del recurso humano-docente a las infraestructuras tecnológicas y redes de computadoras en el C.R.U de Veraguas

Authentication mechanisms for access of human-teaching resources to technological infrastructures and computer networks at the C.R.U of Veraguas

Oscar E. Rodríguez C.[1], Raúl E. Dutari D.[2], David A. Rodríguez F.[3], Libertad Fernández G.[4], Juan G. Quintero P.[5], Humberto J. Chang M.[6]

[1]Universidad de Panamá, Facultad de Informática, Electrónica y Comunicación, Panamá; oseroca.rodriguez@up.ac.pa; https://orcid.org/0000-0001-5438-8037
[2]Universidad de Panamá, Facultad de Informática, Electrónica y Comunicación, Panamá; raul.dutari@up.ac.pa; https://orcid.org/0000-0002-7954-5999
[3]Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales, Panamá; david.rodriguez12@utp.ac.pa; https://orcid.org/0000-0002-7167-944X
[4]Universidad de Panamá, Facultad de Administración de Empresas y Contabilidad, Panamá; libertad.fernandez@up.ac.pa; https://orcid.org/0000-0002-3705-4761
[5]Universidad de Panamá, Facultad de Informática, Electrónica y Comunicación, Panamá; juan.quinteroo@up.ac.pa; https://orcid.org/0000-0002-7308-2102
[6]Universidad de Panamá, Facultad de Derecho y Ciencias Políticas, Panamá; humberto.chang@up.ac.pa; https://orcid.org/0000-0003-1126-2826

Fecha de recepción: 30 de marzo de 2024 *Fecha de aceptación: 18 de mayo de 2024*

DOI https://doi.org/10.48204/j.vian.v8n1.a5229

Resumen: Con el propósito de identificar las fortalezas y debilidades de los mecanismos de autentificación para el acceso a las infraestructuras tecnológicas que se administran y gestionan bajo el entorno de las redes de computadoras en el Centro Regional Universitario de Veraguas, se aplicó durante los meses de noviembre-diciembre del año 2023, un formulario en línea dirigido de manera remota y con el consentimiento informado, a 373 profesores que forman las 16 facultades en esta unidad académica. El 79.08% (295) respondieron dicho instrumento, el cual recopiló el promedio de los años de servicios académicos y la dedicación docente como elementos generales; y como aspecto concluyente, se determinó que el 93.22% (275) considera muy importante la capacitación técnica del recurso humano-docente, en materia de seguridad para el diseño de contraseñas para el acceso a las infraestructuras tecnológicas y de la aplicación de nuevas políticas de protección de la información para la mejor administración de los métodos de autentificación en el uso de las redes de computadoras.

Palabras clave: infraestructuras tecnológicas, redes de computadoras, mecanismos de autentificación, contraseñas, recursos humanos, capacitación.

Abstract: With the purpose of identifying the strengths and weaknesses of the authentication mechanisms for access to the technological infrastructures that are administered and managed under the environment of computer networks at the Regional University Center of Veraguas, an online form was applied during the months of November-December 2023, directly remotely and with informed consent, to 373 professors who make up the 16 faculties in this academic unit. A percentage of 79.08% (295) responded to this instrument, which collected the average years of academic service and teaching dedication as general elements; and as a

conclusive aspect, it was determined that 93.22% (275) consider the technical training of human-teaching resources to be very important, in terms of security for the design of passwords for access to technological infrastructures and the application of new security policies for the protection of information for better administration of authentication methods in the use of computer networks.

Keywords: technological infrastructures, computer networks, authentication mechanisms, password, human resources, training.

1. Introducción

Desde los albores de la humanidad, el concepto de redes ha jugado un papel fundamental en el desarrollo social y educativo de la sociedad; es por ello que, hoy por hoy, las redes de computadoras se han convertido en el soporte tecnológico de toda la colectividad, cada vez más ávida de los recursos y servicios que se ofrecen, las cuales a través de sus hilos y ondas invisibles, interconectan al mundo por medio de múltiples arterias digitales que son vitales para su funcionamiento y que alimentan las necesidades de datos e información de las personas y organizaciones (Tian y Gao, 2024).

Cada vez más, dependemos de sus intrincados enlaces de conexión de forma física o inalámbrica, lo que se convierte en un viaje de interconectividad sin fronteras, desafiando las distancias y acercando a las personas, objetos y sistemas, a través de una súper telaraña digital de comunicación.

Ciertamente su influencia, importancia y aplicación, llega a cada rincón del orbe, lo que permea a un sinnúmero entidades educativas, siendo la Universidad de Panamá y sus Unidades Académicas, una de ellas.

La Universidad de Panamá, como ente académico en educación superior, cuenta con 10 Unidades Académicas o Centros Regionales Universitarios (CRU, por sus siglas) a nivel nacional (Universidad de Panamá, 2024); por lo que, el CRU de Veraguas, inicia sus funciones, labores y actividades educativas como la Extensión Universitaria de Santiago, establecida bajo la Ley Nº60 del 11 de diciembre de 1961, y como Centro Regional Universitario, según el Decreto de Gabinete Nº144 del 3 de junio de 1970.

Esta Unidad Académica (CRUV, de ahora en adelante), es una instancia de tipo educativa y administrativa de la Universidad de Panamá, la cual está reglamentada por la Ley Nº24 del 14 de julio de 2005 y actualizada a través de la Gaceta Oficial Nº25344 del 18 de julio de 2015 y del Estatuto Universitario, aprobado en el Consejo General Universitario,

Nº22-08 del 29 de octubre de 2008, promulgado en la Gaceta Oficial Nº26202 del 15 de enero de 2009 y en su última modificación publicada en Gaceta Oficial Nº28791 del 7 de junio de 2019; y normas generales y específicas de la institución establecidas para los Centros Regionales Universitarios, las cuales establecen el marco que reglamenta las cinco actividades sustantivas que se desarrollan en esta entidad académica: docencia, investigación, extensión, producción y servicio.

Transcurridas más de 5 décadas desde su creación, esta Unidad Académica ha incrementado vertiginosamente la matrícula de estudiantes (Universidad de Panamá, 2024); por ende, también refleja un notorio aumento en la planta docente. Esto se evidencia a través de la presencia y funcionamiento de 16 facultades (de un total de 18), que administran alrededor de 38 carreras universitarias, las cuales son atendidas por 411 docentes y 153 funcionarios administrativos (Secretaría Académica (CRUV), 2023).

Bajo otro escenario, es evidente que, a raíz de la pandemia de 2020, muchas actividades y servicios sociales, comerciales, económicas y sobre todo educativas (en todos sus niveles de escolaridad), cambiaron y se transformaron producto de la omnipresencia de las tecnologías de la información y comunicación, redes de computadoras, sistemas de transmisión de datos, recursos web y ahora, con la presencia de las tecnologías emergentes, como la Inteligencia Artificial. Ciertamente, hemos sentido de forma directa su influencia, ya que esta situación nos afectó totalmente como sociedad y como miembros de las entidades donde prestamos servicios y desarrollamos nuestra labor profesional.

Por lo antes expuesto, la Universidad de Panamá como actor educativo a nivel superior, se encaminó hacia la utilización masiva y abierta de sus infraestructuras tecnológicas (aplicaciones web, plataformas educativas, redes de computadoras y sistemas académicos-administrativos, entre otros), para estudiantes, docentes y administrativos en este periodo; lo que permitió cubrir las necesidades emergentes y subsanar poco a poco los inconvenientes educativos que se presentaron en ese momento y bajo circunstancias puntuales.

Esto ha ocasionado un aumento considerable en el número de usuarios (estudiantes, profesores y administrativos), que utilizan y dependen cada vez más de dichas

infraestructuras tecnológicas; y que, a su vez son necesarias para la gestión académica y administrativa de la institución. Sin embargo, un problema que surge a raíz de esta situación se entrelaza y vincula con el acceso a los servicios (bibliotecas virtuales, correo institucional y sistemas de talonarios, entre otras) y las aplicaciones educativas (plataforma UPVirtual, E-ducativa, sistema de evaluación y servicios docentes) que se ofrecen sobre éstas; lo que hace justo y necesario el estudio de métodos de autentificación para el acceso del recurso humano-docente que requieren de estos servicios.

Un mecanismo de autentificación, es un proceso que incluye un conjunto de procedimientos y protocolos, diseñados para verificar la identidad de un usuario que desea o intenta acceder a través de un equipo informático o dispositivo electrónico a una red de computadoras (Pfleeger, et al., 2024).

De igual forma es muy importante destacar que, el objetivo principal de este proceso es el de garantizar, proteger y asegurar que sólo los usuarios registrados a estas infraestructuras tecnológicas puedan ingresar a través de una contraseña segura a las redes de computadoras, protegiendo así la confidencialidad, integridad y disponibilidad de la información académica y administrativa (BoonKrong, 2021).

Destaca Martínez, (2021) que, la resistencia y confiabilidad de las contraseñas son aspectos cruciales que deben considerarse cuidadosamente, ya que de ellas depende la seguridad para el acceso a las infraestructuras tecnológicas, redes de computadoras y los sistemas informáticos institucionales y empresariales; así como también de sus cuentas, tanto a nivel personal como profesional.

Aunado a lo anterior, en los últimos años hemos sido testigos de un vertiginoso y exponencial crecimiento en la utilización de la red Internet, así como en la exploración de sus recursos y aplicaciones, que día a día aparecen y acaparan la atención de los usuarios (International Telecommunication Union, 2024). Este auge, sin embargo, ha traído consigo un aumento significativo en la incidencia de ataques e intrusiones dirigidos a servicios que se administran sobre las diversas infraestructuras tecnológicas y que gestionan sus aplicaciones a través de las redes de computadoras, con el claro propósito de obtener

información confidencial de usuarios y de organizaciones públicas y privadas; siendo las instituciones educativas de nivel superior, una de ellas (Grimes, 2021).

Bajo este escenario tecnológico digital, resalta la urgente necesidad de implementar medidas de seguridad sólidas y efectivas para contrarrestar las crecientes amenazas y detectar puntos vulnerables; por lo que, en este contexto, las contraseñas juegan un papel fundamental como primera barrera de seguridad y anillo de protección del recurso humano-docente que labora en el CRUV.

Cabe señalar que, es imperativo conocer el diseño, la estructuración y usabilidad de las contraseñas por parte de los docentes de esta Unidad Académica, las cuales se han vuelto un componente esencial en la salvaguarda de la integridad de la información institucional-académica (López y Villa, 2016).

Por lo antes expuesto, la importancia de este enfoque de seguridad radica en la prevención de situaciones comprometedoras que podrían derivar en la filtración de datos sensibles de tipo académico, pérdida de privacidad o incluso, en el acceso no autorizado a los sistemas, servicios y cuentas de usuario del recurso humano-docente, que se administran en el CRUV.

El objetivo principal de este estudio consiste en identificar los criterios empleados por el recurso humano-docente para la creación, uso y respaldo de contraseñas como elementos de seguridad para el acceso a las infraestructuras tecnológicas y redes de computadoras; las cuales constituyen el medio tecnológico para la gestión de los servicios y actividades académicas-administrativas que demandan un control de acceso.

En resumen, la importancia de la implementación de buenas prácticas de seguridad, se erigen como pilares fundamentales sobre los principios técnicos y científicos para el establecimiento de contraseñas seguras; los cuales se posicionan como una estrategia fundamental de seguridad para el acceso a los servicios y recursos proporcionados por el CRUV a todo el cuerpo de recurso humano-docente que labora en la institución.

2. Materiales y métodos

En el último lustro, la matrícula de estudiantes que incluye los de primer ingreso y reingreso en el CRUV, se ha incrementado en un 19,45% (Universidad de Panamá, 2024), lo que también ha significado un aumento del 4.85%, en la contratación de nuevo recurso humano-docente (Secretaría Académica (CRUV), 2023), para cumplir con la gran demanda de la población estudiantil.

Por otro lado, para desarrollar el proceso de recopilación de la información, se diseñó y elaboró un instrumento con 10 interrogantes de selección múltiple; el cual se aplicó a través de un formulario electrónico en línea de forma remota, utilizando como medio de enlace el correo institucional de los docentes, bajo la condición privada de consentimiento informado, al 90.7542% de la población de profesores especiales y regulares con dedicación de tiempo parcial y tiempo completo (373 de un total de 411), que actualmente se encuentran en la organización docente del segundo semestre del año académico 2023.

Según Sallis, et al. (2021), la definición y uso del término de población, implica en su totalidad hacer referencia a los sujetos seleccionados de estudio; por lo que, se define como la colección completa de todos los elementos a estudiar. Sin embargo, Hernández-Sampieri y Mendoza Torres, (2018), definen el concepto de población como el conjunto de elementos o individuos que poseen ciertas características o particularidades, sobre los cuales se busca realizar deducciones, o bien, componen la unidad de análisis del estudio.

Sin duda, al tener información sobre la población encuestada, se simplifica y al mismo tiempo, posibilita la realización de cálculos matemático-estadísticos para determinar la muestra, conforme a la cantidad de profesores previamente mencionada. Bernal (2016) destaca que, una muestra es un subconjunto representativo de individuos, elementos o unidades que son seleccionados de una población más grande con el propósito de realizar observaciones, mediciones o análisis.

Existen varios métodos estadísticos disponibles para determinar y establecer el tamaño adecuado de la muestra, cuando se conoce el total de la población que debe ser extraída de la cantidad de profesores encuestados; por lo que, se aplica el procedimiento a través de las siguientes fórmulas:

$$1. \quad n' = \frac{P(1-P)}{V^2} = \frac{P(1-P)}{(se)^2}$$

$$2. \quad n = \frac{n'}{1 + \frac{n'}{N}}$$

$$3. \quad S = se = V$$

Fuente: Hernández-Sampieri y Mendoza Torres, 2018.

Donde:

$n' =$ Tamaño de la muestra sin ajustar.

$n =$ Tamaño de la muestra ajustada.

$N = 411$ Población total.

$se = 0.05 = 5\% =$ Error estándar establecido por los investigadores.

$P = 0.5 = 50\% =$ Probabilidad de ocurrencia de que el elemento seleccionado en la población, presente el atributo de interés en la encuesta (sin premuestreo) (Triola, 2018).

$V^2 =$ Varianza de la población a encuestar.

$S^2 =$ Varianza de la muestra.

Sustituyendo los valores conocidos, se obtiene:

$$n = 80.4305 \approx 81$$

Es relevante mencionar que se obtuvieron respuestas de 295 profesores y profesoras, lo que equivale al 79.0885% de la población total investigada. Esto implica que se debe seleccionar al menos a 81 docentes de los 411 miembros de la población total para realizar un muestreo representativo. Por lo tanto, dado que el cuestionario fue contestado por 295 docentes, se puede concluir que el tamaño mínimo de la muestra es inferior a la cantidad de profesores que participaron en el estudio.

Esto indica que se utilizará un tamaño de muestra mayor al mínimo requerido, situación que se describe de la siguiente manera:

$$\#(PT) = 411,\ \#(TMM) = 81,\ \#(PE) = 295,\ \#(PC) = 373$$

$$\therefore$$

$$\#(TMM) \leq \#(PE) \leq \#(PC) \leq \#(PT)\ \wedge\ \forall p_{TMM} \in \{TMM\},\ p_{TMM} \in \{PE\}$$

Donde:

$PT =$ Conjunto de la población total de profesores (411).

$PC =$ Conjunto de profesores consultados (373).

$TMM =$ Conjunto de profesores que tiene el tamaño mínimo de muestra (81).

$PE =$ Conjunto de profesores encuestados (295).

$p_{TMM} =$ Un profesor cualquiera que colaboró con la investigación, respondiendo la encuesta aplicada.

El formulario se diseñó con 10 ítems de tipo selección múltiple, el cual fue validado a través del coeficiente alfa de Cronbach, utilizando la siguiente fórmula matemática:

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum_{i=1}^{k} \sigma_i^2}{\sigma_x^2}\right)$$

$$\alpha = 0.81$$

k = Número de items del formulario.

σ_i^2 = Varianza de cada items.

σ_x^2 = Variana total de las puntuaciones de cada items.

Es significativo recalcar que, el diseño y la estructura del formulario fue concebido para evitar inconvenientes y garantizar practicidad y facilidad de cumplimentación; dado que no se disponía de información sobre las condiciones y el nivel de habilidades tecnológicas de los encuestados, por lo que se priorizó la rapidez en la respuesta; por lo tanto, el diseño permitía una navegación ágil y una selección de respuestas sencilla en cada pregunta, sin comprometer la experiencia del usuario.

Dicho instrumento se estructuró en una sola sección, en la cual los 2 primeros items se vinculaban al rango de años de servicios académicos en la Universidad de Panamá y su dedicación como docente, las cuales representaban el (20.0%) de los datos generales de los encuentados; por otro lado, 8 (80.0%) de los items restantes, está vinculada a determinar los servicios a nivel institucional que con frecuencia utiliza, las particularidades y diseño de

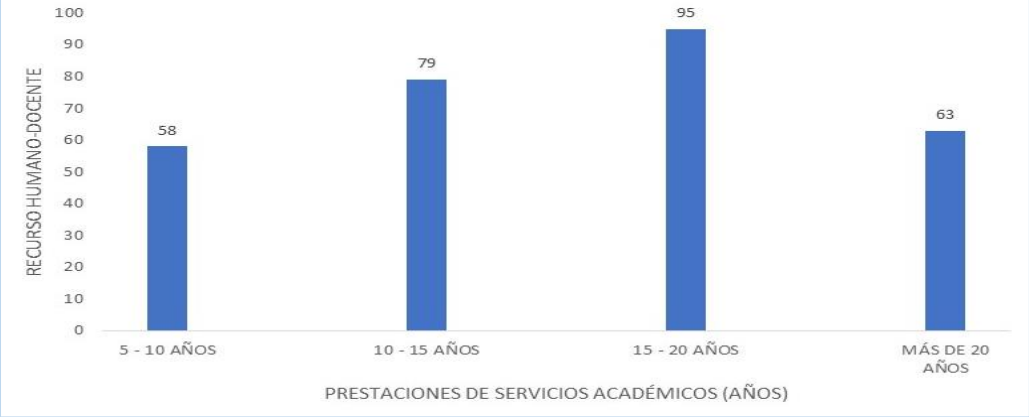
las contraseñas utilizadas para el acceso a dichos servicios y quizas lo más importante, la necesidad de planificar, organizar y desarrollar jornadas de capacitación en materia de políticas de seguridad aplicadas a la generación de contraseñas.

3. Resultados

Los resultados obtenidos mediante la aplicación del formulario en línea, posibilitan el análisis de los datos recopilados; por consiguiente, se incluye en la Figura 1, la categorización del rango de años de acuerdo a la hoja de prestaciones de servicios académicos de los profesores encuestados, destacándose como uno de los aspectos fundamentales en el estudio.

Figura 1

Años de prestaciones de servicios académicos.



Es importante enfatizar que, 174 (58.98%) del recurso humano-docente cuenta con los suficientes años de servicios (entre 10 a 20 años) dentro de la Universidad de Panamá, lo que facilita un espectro amplio en el conocimiento de esta institución de educación superior.

Asimismo, en conexión con la pregunta anterior, se investigó la dedicación docente dentro de la Universidad de Panamá, cuya representación se muestra en la Figura 2.

Figura 2

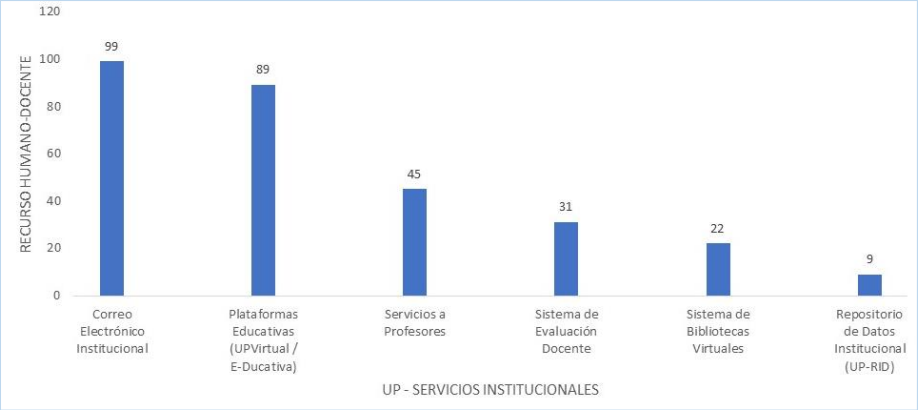
Dedicación docente, según su organización académica.

Los resultados derivados destacan que, los 202 (68.47%) del recurso humano-docente encuestados, ya cuentan con una posición sobre el nombramiento por resolución, lo que permite tener cierta experiencia bajo el contexto académico-administrativo en el CRUV. De igual manera, los 93 (31.52%) docentes, poseen dedicación a tiempo completo, lo que facilita aún más conocer esta unidad académica y su funcionamiento.

Por otro lado, en la figura 3 se presentan los resultados obtenidos de la frecuencia y uso de los servicios institucionales que brinda la Universidad de Panamá, a todo el claustro del recurso humano-docente, como soporte a las actividades educativas a nivel superior. Cabe señalar entonces que, en los primeros lugares están el correo electrónico institucional 99 (33.55%), y luego le sigue las plataformas educativas 88 (29.83%); lo que denota una relación directa entre estos servicios, ya que, a través del correo se realiza el proceso de inscripción del estudiante en el aula y también lo concerniente al registro de actividades educativas (Foros, Laboratorios, Parciales, entre otros) y el control de la evaluación general en las asignaturas de cada docente.

Figura 3

Servicios Institucionales.

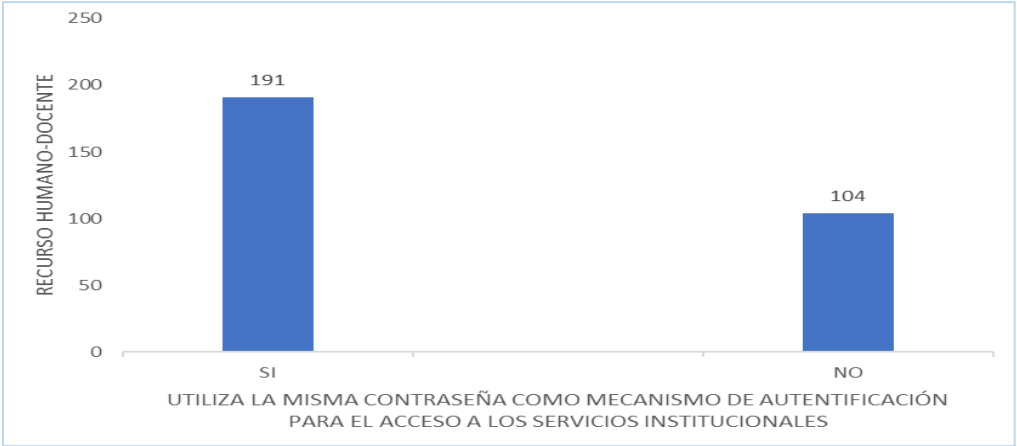


También es muy importante señalar que, los servicios de menor usabilidad le corresponden al sistema de bibliotecas virtuales con 22 (7.45%) y los repositorios de datos 9 (3.05), tópicos que son vitales y de gran ayuda para la realización de investigaciones y trabajos educativos, para docentes y discentes en el CRUV.

Entrando en más detalles sobre el mecanismo de autentificación para acceso a los diversos servicios institucionales y redes de computadoras que son utilizadas por el recurso humano-docente para el desarrollo de sus tareas académicas-administrativas, llegamos al punto de señalar que en la figura 4, se presenta 191 (64.74%) utiliza la misma contraseña como elemento de seguridad para la entrada a dichos servicios; razón que denota un punto vulnerable en materia de protección y salvaguarda de la información que se gestiona a través de dichos servicios.

Figura 4

Mecanismo de autentificación para el acceso a los servicios institucionales.



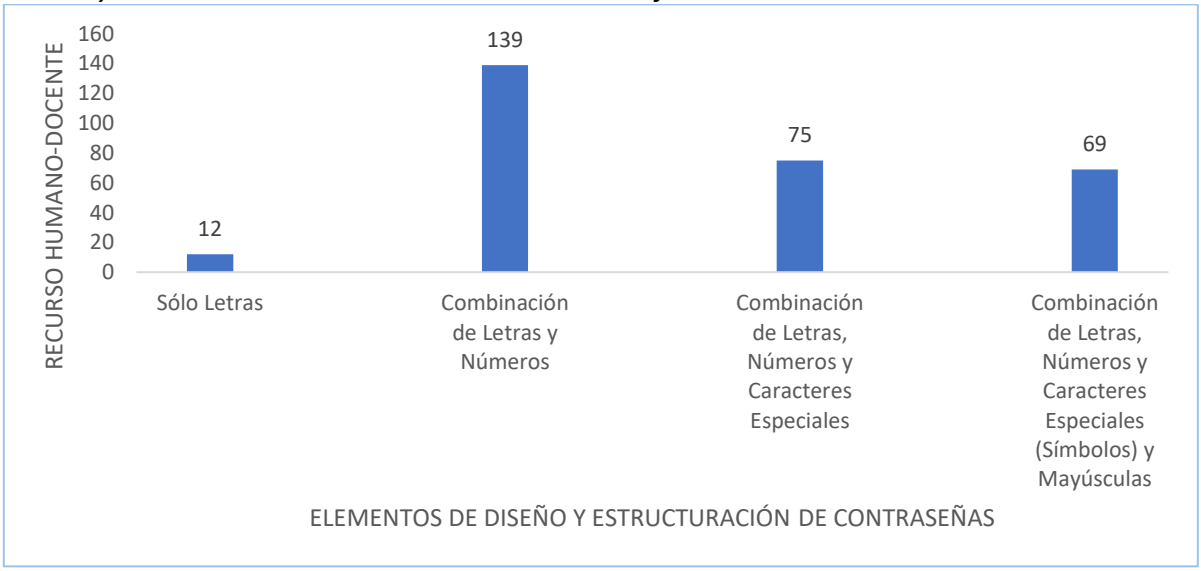
Reiterando lo expuesto por Dash (2023), las contraseñas se convierten en el punto inicial más vulnerable para el acceso a los sistemas y redes de computadoras, lo que, al asociarlo con los resultados obtenidos, enciende las alarmas en materia de seguridad y protección de la información académica del recurso humano-docente que utiliza día a día estos servicios y recursos de la institución.

En el mismo orden de ideas de la pregunta anterior, se indagó sobre el diseño y estructuración del mecanismo de autentificación para el acceso a las infraestructuras tecnológicas que brindan los servicios académicos-administrativos del CRUV, lo que dio como resultados los datos obtenidos en la figura 5.

Un aspecto a destacar en primera instancia que se observa en dicha figura, se vincula a que 139 (47.11%) del recurso humano-docente, utiliza como elementos para el diseño y estructuración del mecanismo de autentificación, la combinación de letras y números, lo cual no resulta difícil de comprender; ya que, son elementos básicos que exigen algunos de los servicios institucionales que se manejan actualmente.

Figura 5

Diseño y Estructuración de Mecanismos de Autentificación.



También se puede indicar que, sólo 69 (23.38%) del recurso humano-docente, diseña y estructura su mecanismo de autentificación cumpliendo parámetros técnicos más adecuados en materia de seguridad; lo que marca un precedente para proponer jornadas de capacitación académica en este aspecto.

Como una cadena de eventos que inciden de forma directa en las diversas circunstancias en una situación particular, se suma a lo antes expuesto, el análisis de los periodos de tiempo que aplica el recurso humano-docente para hacer cambios o ajustes en los mecanismos de autentificación, lo cual se presenta la figura 6.

Figura 6

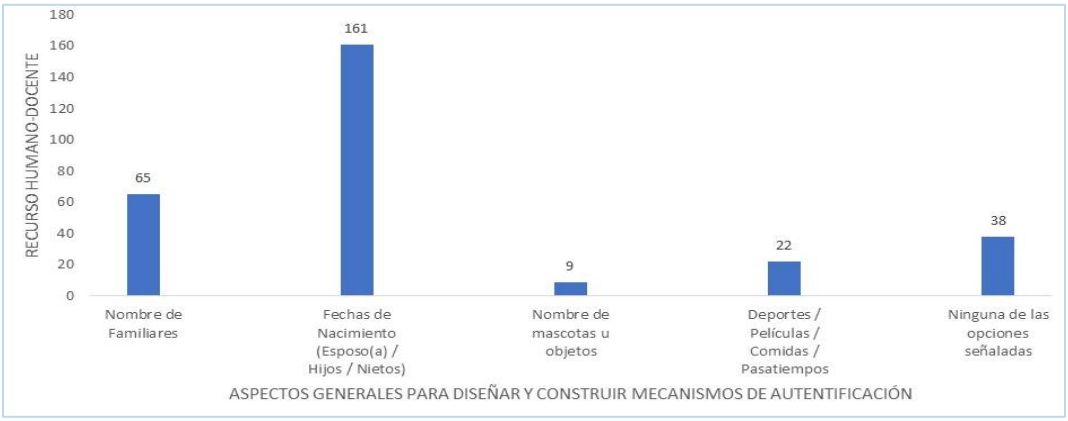
Periodo de tiempo para el cambio del mecanismo de Autentificación.

De la figura anterior se puede observar que, los resultados obtenidos tienen una relación directa, puesto que 148 (50.16%) de los encuestados, cambian su mecanismo de autentificación cuando el sistema así lo solicite; razón que se suma al conjunto de factores que pueden desencadenar un tsunami de inconvenientes para el acceso a los servicios institucionales y redes de computadoras.

Por otro lado, se investigó más afondo sobre los aspectos o elementos que utiliza el recurso humano-docente para construir los mecanismos de autentificación, lo cual dio como resultados lo que se muestra en la figura 7.

Figura 7

Aspectos generales para diseñar y construir mecanismos de autentificación



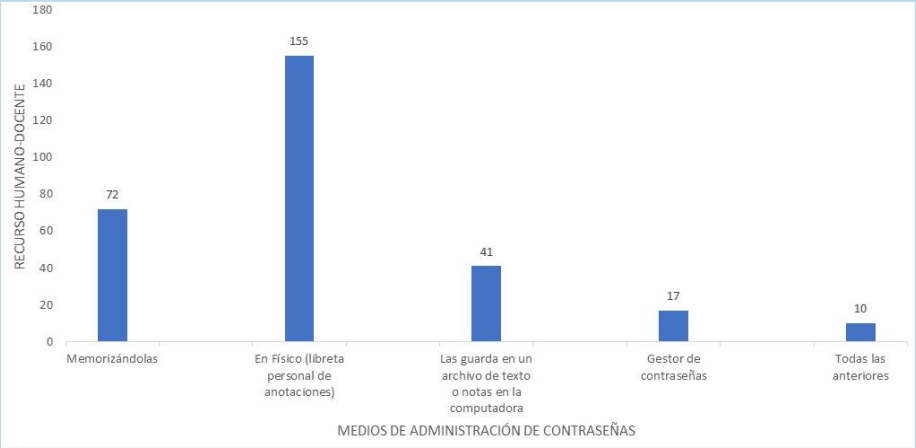
De la figura expuesta se destaca que, 161 (54.57%) de los profesores utilizan fechas de nacimiento de familiares para diseñar y construir mecanismos de autentificación, y si agregamos que, 65 (22.03%) aplica nombres de familiares para el mismo caso, demuestra un alto grado de malas prácticas aplicadas a la seguridad en el acceso de las infraestructuras tecnológicas antes señaladas, que brindan los servicios académicos-administrativos del CRUV.

Ciertamente en el análisis de los resultados obtenidos, aparecen más elementos que enfatizan la grave situación que atravesamos en materia de seguridad, protección, privacidad y confidencialidad de la información en el contexto académico.

Poco seguimos avanzando en el análisis de los resultados obtenidos a través de la aplicación del instrumentos en línea, del cual señalamos que, en la figura 8 se muestran los datos que destacan la forma en que el recurso humano-docente administra sus contraseñas como mecanismos de autentificación para el acceso a las infraestructuras tecnológicas de la Unidad Académica objeto de estudio, de los cuales 155 (52.54%) docentes, resguardan su información de acceso en físico (liberta personal de anotaciones), y si agregamos que 41 (13.89%) las guarda en un archivo de texto o notas en la computadora, tenemos un elevado número de docentes que esta propenso a pérdida de su información de acceso, producto de procedimientos no adecuados para dicho resguardo de su información.

Figura 8

Medios de resguardo y administración de contraseñas



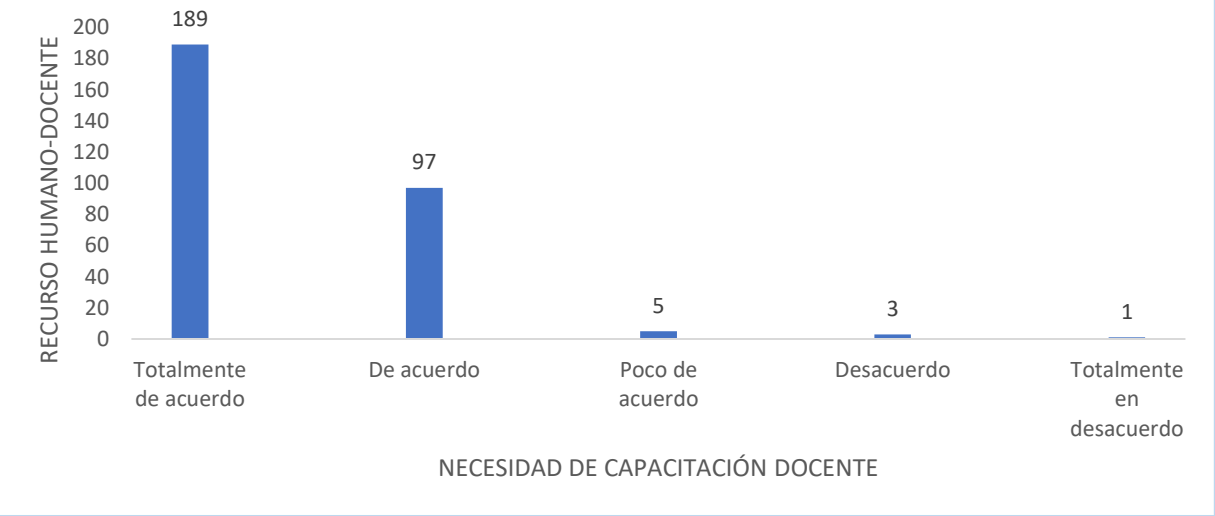
Un aspecto fundamental en este punto y que vale la pena señalarlo es que, 17 (5.76%) del recurso humano-docente, utiliza gestores de contraseñas como tecnología de seguridad

para el acceso a las infraestructuras tecnológicas y redes de computadoras de la institución; lo que hace aplicar un elemento adicional de protección en el proceso.

Todo lo antes expuesto presenta un enorme problema en materia de seguridad y protección de la información que el recurso humano-docente, utiliza como medio de acceso a los servicios y recursos de la unidad académica; por lo que, en la figura 9, se presentan los resultados de la pregunta más importante aplicada a dichos docentes, la cual hace referencia a la necesidad de planificar , organizar y desarrollar jornadas de capacitación docente en materia de seguridad y protección de la información confidencial que utiliza dicho personal para acceder a dichas infraestructuras tecnológicas y redes de computadoras.

Figura 9

Necesidad de capacitación docente



El recurso humano-docente respondió fuerte y claro, ya que siente la necesidad de capacitarse como actividad académica y profesional; por lo que 189 (64.06%) señalo estar totalmente de acuerdo con realizar jornadas de perfeccionamiento, y si agregamos que 97 (32.88%) lo reforzo a través de estar de acuerdo con esta actividad.

Como fase conclusiva del estudio, se han compartido los resultados derivados de la aplicación del formulario en línea de manera remota, tras obtener el consentimiento informado del recurso humano-docente del CRUV, quienes desempeñan un papel crucial en el desarrollo del proceso de enseñanza y aprendizaje a nivel superior. Cabe señalar que, dichos resultados han sido presentados con el propósito de proporcionar una base

sustancial para el análisis y la discusión del tema de investigación, brindando los argumentos fundamentados y las explicaciones detalladas para respaldar y contextualizar los hallazgos presentados, con el objetivo de facilitar una comprensión exhaustiva y precisa de los mismos.

4. Discusión

Los servicios y recursos académicos-administrativos que se gestionan a través de las distintas infraestructuras tecnológicas y se administran sobre las redes de computadoras del CRUV, y que son las herramientas indispensables para el quehacer del recurso humano-docente, juegan un papel fundamental en el desarrollo de las actividades educativas que sustentan el proceso de enseñar y de aprender; por ello, se hace vital comprender la importancia del diseño, estructuración y la correcta utilización de los mecanismos de autentificación para el acceso a estas aplicaciones tecnológicas.

Destaca Smith-Creasey (2024), los mecanismos de autentificación tienen defectos bien conocidos, los cuales principalmente dependen de como los usuarios las diseñen y utilicen para el acceso a sus equipos informáticos y dispositivos tecnológicos modernos; y que, a su vez, son utilizados en múltiples aparatos.

Queda claro que, cada día dependemos más y más de dichos equipos para ejecutar nuestras tareas diarias y que necesitamos de las contraseñas como medio de acceso a los mismos; sin embargo, Fanti (2023) señala que, los avances informáticos seguirían en ascenso y las tecnologías de autentificación se desarrollarían cada vez más, por lo que, sería muy probable que de alguna manera siempre se dependa de un secreto que sólo usted conozca, las contraseñas.

Bajo un panorama actualizado y moderno, con la omnipresencia de las tecnologías emergentes, el internet de las cosas y del desarrollo de los recursos y aplicaciones web, se hace imperativo aplicar nuevas estrategias de protección y seguridad en el diseño de las contraseñas que utilizamos diariamente; por ello, señala Liyanage et al. (2020) que, hoy se requiere de soluciones rápidas y de métodos de autentificación y cifrados robustos, que

puedan ser utilizados por cada usuario que así lo requiera como elemento de seguridad principal.

Lo antes expuesto enfatiza que, la utilización de los métodos de autentificación modernos fundamentados en contraseñas, deben ser diseñados y estructurados por los usuarios de manera más técnica y generados a través de aplicaciones de tipo gestores de contraseñas (Papathanasaki et al., 2022); las cuales pueden ser definidas como una aplicación de tipo informática y tecnológica que guarda y almacena las contraseñas de forma cifrada, utilizando las credenciales de inicio de sesión de las cuentas, servicios y recursos de múltiples sitios en la web (Odriozola et al., 2020).

Los resultados derivados del proceso de investigación y las evidencias teóricas referenciadas, sustentan la gran importancia de la aplicación y puesta en práctica de mejores y más eficientes estrategias para el diseño, estructuración y utilización de contraseñas por parte del recurso humano-docente; quienes son los usuarios de las diversas infraestructuras tecnológicas y redes de computadoras que brinda el CRUV, como parte de los servicios y recursos académicos-administrativos.

De igual forma, se hace justo y necesario la planificación, organización, ejecución e implementación de jornadas capacitación académica-técnica, cónsono con las características y competencias del recurso humano-docente del CRUV, que permite el desarrollo de competencias digitales en materia de seguridad y protección de la información académica.

5. Conclusiones

Desde los albores de nuestra civilización, la seguridad ha sido un pilar fundamental para el progreso de la humanidad y la evolución de la sociedad moderna; como el escudo protector que salvaguarda nuestros bienes y la propia existencia, arraigándose profundamente en nuestro ADN. Por lo que, cada decisión que tomamos está impregnada de la búsqueda de seguridad, especialmente en la era digital actual, con la presencia de las tecnologías de la información y comunicación, el internet de las cosas, las tecnologías emergentes y la inteligencia artificial.

De igual manera y de forma invisible e inadvertida, las contraseñas forman parte muy importante de nuestras vidas; ya que no existe actividad, tarea y acción que desarrollamos bajo el escenario tecnológico, en donde su aplicación no esté presente y que sea la llave para acceder a los servicios y recursos que se brinda a través de las infraestructuras tecnológicas y redes de computadoras al recurso humano-docente que desarrolla su praxis docente en el CRUV.

Por su parte, la selección del mecanismo de autenticación más adecuados, dependerá de los requisitos, políticas específicas de seguridad, costos y conveniencias que proponga la Universidad de Panamá a través de la Dirección de Tecnología de la Información y Comunicación, para el recurso humano-docente que labora en cada una de sus Unidades Académicas.

De igual manera, los mecanismos de autenticación basados en contraseñas, siguen siendo ampliamente utilizados debido a su simplicidad y bajo costo; sin embargo, son muy vulnerables a los ataques de fuerza bruta y phishing, lo que destaca la gran necesidad implementar estrategias de seguridad adicionales para mayor conveniencia y seguridad del recurso humano-docente que utiliza los servicios y recursos del CRUV.

Otro escenario fundamental, se vincula con la educación y la concienciación del recurso humano-docente, sobre el uso y aplicación de mejores prácticas de autenticación; las cuales son fundamentales para prevenir el acceso no autorizado.

La Universidad de Panamá, como entidad de educación superior, debe planificar, organizar y proporcionar jornadas de capacitación de forma regular y reforzar la importancia de utilizar contraseñas seguras; ya que año tras año ingresa nuevo recurso humano-docente al CRUV y que necesita utilizar los diversos servicios académicos-administrativos de esta Unidad Académica.

Para finalizar, al implementar mecanismos de autenticación integrales y promover nuevas y mejores prácticas de seguridad basadas en contraseñas, el CRUV, estaría en mejor posición para garantizar el acceso seguro de su recurso humano-docente, a las infraestructuras tecnológicas y redes de computadoras, protegiendo así sus valiosos recursos y datos académicos.

Referencias Bibliográficas

Bernal Torres, C. (2016). Metodología de la investigación: administración, economía, humanidades y ciencias sociales (Cuarta ed.). Pearson Educación.

BoonKrong, S. (2021). Authentication and Access Control. Apress. https://www.mcu.edu.ng/home/wp-content/uploads/2023/11/Authentication-And-Access-Control-Practical-Cryptography-Methods-And-Tools-by-Sirapat-Boonk rong-z-lib.org-1.pdf

Dash, S. (2023). Ultimate Web Authentication Handbook. Orange Education.

Fanti, M. (2023). Implementing Multifactor Authentication: Protect your applications from cyberattacks with the help of MFA. Packt Publishing.

Grimes, R. A. (2021). Hacking Multifactor Authentication. John Wiley & Sons.

Hernández-Sampieri, R., & Mendoza Torres, C. P. (2018). Metodología de la Investigación (Las rutas cuantitativa, cualitativa y mixta). McGraw-Hill. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf

International Telecommunication Union [ITU]. (2024, 12 febrero). Statistics. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Liyanage, M., Braeken, A., Kumar, P. & Ylianttila, M. (2020). IoT Security. John Wiley & Sons.

López Echeverry, A. M., & Villa Sánchez, P. A. (2016). Política de gestión de contraseñas para usuarios finales. Scientia Et Technica, 21(01), 7. https://doi.org/10.22517/23447214.8867

Martínez S., G. (2021). Herramientas para la Ruptura del Secreto de Contraseñas. [Trabajo de Fin de Carrera/Grado, Universidad Politécnica de Madrid]. Archivo Digital UPM. https://oa.upm.es/68583/

Odriozola, M., da Silva, N., Puk, I., Poveda, D. y Pavon, L. (2020). Análisis y comparación sobre gestores de contraseñas. En V. C. CoNaIISI (Ed.). Universidad Nacional de San Francisco.https://grupogemis.com.ar/wpcontent/uploads/2021/12/Gestores_Contrasenas.pdf

Papathanasaki, M., Maglaras, L., & Ayres, N. (2022). Modern Authentication Methods: A Comprehensive Survey. AI, Computer Science and Robotics Technology, 2022(0), 1-24. http://dx.doi.org/10.5772/acrt.08

Pfleeger, C., Pfleeger, S., & Coles-Kemp, L. (2024). Security In Computing (Sixth ed.). Pearson Education.

Sallis, J., Gripsrud, G., Olsson, U., & Silkoset, R. (2021). Research Methods and Data Analysis for Business Decisions: A Primer Using SPSS. Springer. https://www.springerprofessional.de/en/research-methods-and-data-analysis-for-business-decisions/19814818

Secretaría Académica (CRUV). (2023). Estadísticas I-II Semestre. Universidad de Panamá.

Smith-Creasey, M. (2024). Continuous Biometric Authentication Systems (An Overview). Springer. https://www.springerprofessional.de/en/continuous-biometric-authentication-systems/26611584

Tian, Y.-C., & Gao, J. (2024). Network Analysis and Architecture. Springer. https://www.springerprofessional.de/en/network-analysis-and-architecture/26113668

Triola, M. (2018). Estadística (Décimosegunda ed.). Pearson Educación.

Universidad de Panamá [UP]. (2024, 16 de marzo). Boletín Informativo (UP). https://up.ac.pa/transparencia/boletinInformativo

Universidad de Panamá [UP]. (2024, 17 de enero). Centros Regionales y Extensiones. https://up.ac.pa/regionales