UNIVERSIDAD NACIONAL DE CAAGUAZÚ
FACULTAD DE CIENCIAS Y TECNOLOGÍAS
CARRERA DE INGENIERÍA EN INFORMÁTICA

PROYECTO FINAL DE GRADO[1]

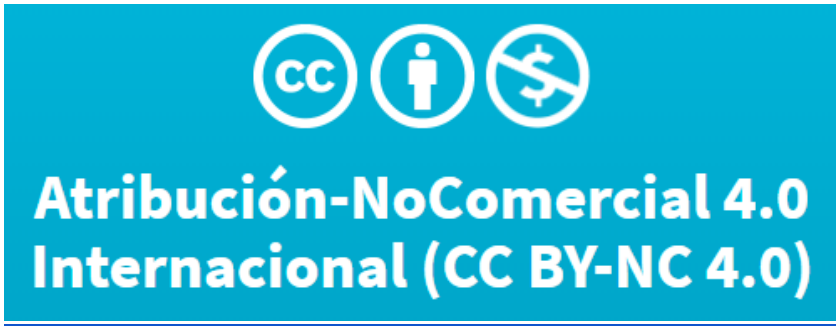
Políticas de seguridad en Sistemas de Información para el rectorado de la Universidad Nacional del Caaguazú en el año 2017

AUTOR: JUSTINO RODRIGO ROJAS SARTORIO

TUTOR: PROF VICTOR MANUEL MELGAREJO RIVEROS

CORONEL OVIEDO, DICIEMBRE DE 2018

[1] Reescrito para adaptarse al formato 2022 de Proyecto Final de Grado.



Usted es libre de:

- **Compartir — copiar y redistribuir el material en cualquier medio o formato**
- **Adaptar — remezclar, transformar y construir a partir del material**

Bajo los siguientes términos:

- **Atribución — Usted debe dar crédito de manera adecuada, brindar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciante.**
- **NoComercial — Usted no puede hacer uso del material con propósitos comerciales.**

RESUMEN

Este trabajo analiza el estado de la seguridad de la información en el Rectorado de la Universidad Nacional del Caaguazú, evaluando las prácticas actuales y proponiendo políticas de seguridad alineadas con el Plan Nacional de Ciberseguridad. La investigación reveló que el rectorado enfrenta serias deficiencias en la gestión de sus sistemas de información, incluyendo una infraestructura tecnológica obsoleta y la falta de políticas de seguridad formales. Además, se encontró que la mayoría del personal y los estudiantes no poseen capacitación en ciberseguridad, lo que incrementa la vulnerabilidad frente a amenazas externas e internas.

El estudio, de tipo descriptivo y analítico, empleó un enfoque cuantitativo-cualitativo para obtener una visión integral de las prácticas y percepciones en torno a la seguridad de la información. Los datos recolectados a través de cuestionarios, observación directa e entrevistas permitieron identificar áreas críticas, como la baja frecuencia en la actualización de contraseñas, el uso limitado de firewalls y antivirus, y el desorden en la instalación y mantenimiento de los equipos. Estas deficiencias exponen a la institución a riesgos significativos, como accesos no autorizados y pérdida de datos sensibles.

Entre las recomendaciones se destacan la implementación de un programa de capacitación en ciberseguridad, la formalización de políticas de seguridad alineadas con los estándares ISO 27001, y la mejora de la infraestructura tecnológica. Asimismo, se sugiere la creación de un Comité de Ciberseguridad, encargado de supervisar y evaluar las medidas implementadas y de fomentar una cultura de seguridad entre los usuarios.

Este trabajo concluye que la adopción de estas medidas es esencial para proteger los activos digitales de la universidad y asegurar un entorno seguro para el desarrollo de sus actividades académicas y administrativas. La implementación de un plan integral de seguridad contribuirá a la sostenibilidad y al fortalecimiento de la institución en el ámbito digital.

Palabras clave:

- *Tecnologías para la Información y la Comunicación (TIC)*
- *ODS 4 - Educación de Calidad*
- *ODS 9 - Industria, Innovación e Infraestructura*
- *ODS 16 - Paz, Justicia e Instituciones Sólidas*

Contenido

INTRODUCCIÓN

La seguridad de la información se ha convertido en un pilar fundamental dentro de la gestión organizacional, especialmente en instituciones educativas, donde la digitalización de datos y el acceso a sistemas informáticos son cada vez más frecuentes. En este contexto, el presente trabajo se enfoca en analizar y proponer mejoras en las políticas de seguridad de la información del Rectorado de la Universidad Nacional del Caaguazú (UNCA). El rápido avance en las tecnologías de información y comunicación (TIC) y el uso extendido de Internet han permitido a las universidades, como la UNCA, facilitar el acceso a datos relevantes y acelerar procesos administrativos y educativos. Sin embargo, este progreso también implica nuevos desafíos de seguridad que, si no se gestionan adecuadamente, pueden poner en riesgo tanto la información como la estabilidad de las operaciones institucionales.

Actualmente, la protección de datos en universidades enfrenta problemas complejos, tales como la falta de infraestructura adecuada y protocolos de seguridad claros, la capacitación limitada del personal en ciberseguridad, y el uso insuficiente de herramientas tecnológicas que garanticen la integridad y confidencialidad de la información. Según Torres-Berrio (2012), el entorno de riesgo en los sistemas de información ha evolucionado sustancialmente, y ahora es indispensable para las organizaciones educativas implementar políticas efectivas de seguridad. Esta necesidad se evidencia en incidentes como el acceso no autorizado a bases de datos, la pérdida de información crucial, y la vulnerabilidad ante ciberataques, que pueden afectar tanto a la comunidad universitaria como a la reputación de la institución. Para abordar estas preocupaciones, se requiere de una estructura formal de seguridad que abarque tanto los recursos físicos como los lógicos de los sistemas, contemplando los estándares internacionales y los lineamientos específicos del Plan Nacional de Ciberseguridad en Paraguay.

Los estudios previos en este ámbito revelan que la gestión de la seguridad de la información en instituciones educativas es un campo relativamente reciente y en crecimiento. En muchos casos, estas instituciones no cuentan con protocolos robustos ni personal especializado en seguridad informática, lo que agrava el riesgo de sufrir ataques. Torres-Berrio (2012) señala que la implementación de redes interconectadas ha potenciado la productividad en las organizaciones educativas, pero también ha aumentado su exposición a amenazas. Esto subraya la importancia de aplicar marcos normativos y operativos, como el estándar ISO 27001, que brindan una metodología clara para evaluar y mejorar los sistemas de seguridad en función de las vulnerabilidades detectadas.

La Universidad Nacional del Caaguazú, como muchas otras instituciones de educación superior en Paraguay, enfrenta una situación crítica en términos de protección de sus activos digitales y sistemas de información. La ausencia de un marco formal y estructurado de políticas de seguridad en la institución ha dado lugar a un entorno de riesgo elevado. Entre los principales problemas se encuentran la falta de supervisión de acceso a la red y al sistema, el desconocimiento de buenas prácticas en el manejo de contraseñas, la exposición a malwares y virus a través de dispositivos de almacenamiento extraíbles y correos electrónicos no verificados, así como la falta de actualización

en los sistemas operativos y software empleados por el personal. Este panorama pone en relieve la necesidad de implementar políticas que aborden estos aspectos y de llevar a cabo una capacitación continua a todos los usuarios involucrados, desde personal administrativo hasta el estudiantado.

A fin de mejorar la situación actual, el objetivo principal de esta investigación es evaluar el estado de la seguridad de la información en el Rectorado de la Universidad Nacional del Caaguazú y desarrollar una propuesta de políticas de seguridad que contribuya a reducir los riesgos informáticos. Este trabajo incluye un análisis detallado de la infraestructura tecnológica y de las capacidades de los usuarios respecto a las amenazas cibernéticas, así como una evaluación de las posibles áreas de mejora en el acceso, uso y gestión de la información dentro del rectorado. Además, se espera que los resultados obtenidos puedan servir como modelo de referencia para otras instituciones educativas del país que enfrenten problemáticas similares y busquen garantizar un entorno seguro para sus operaciones.

El objetivo principal de este trabajo es establecer un modelo de políticas de seguridad de la información dentro del Rectorado de la Universidad Nacional del Caaguazú, basado en el Plan Nacional de Ciberseguridad. Este estudio busca evaluar el estado actual de la seguridad de la información en la universidad, identificar sus principales vulnerabilidades y proponer un conjunto de políticas que garanticen la protección adecuada de los datos institucionales. Para lograrlo, se analizará la infraestructura tecnológica de la UNCA, se evaluarán las prácticas de seguridad actuales y el nivel de conocimiento en ciberseguridad entre los usuarios, con el fin de reducir los riesgos informáticos y mejorar la protección de la información en todos los niveles.

Entre los principales problemas que enfrenta la UNCA se encuentran la falta de protocolos de seguridad estructurados, la capacitación insuficiente del personal en ciberseguridad, y la exposición a amenazas externas debido a la vulnerabilidad de sus sistemas. Estas deficiencias han creado un entorno de alto riesgo, por lo que es esencial implementar políticas de seguridad que aborden aspectos como el acceso a los sistemas, el manejo de contraseñas y la protección frente a ciberataques.

Este trabajo también tiene como objetivos específicos:

1. Describir las actividades susceptibles a la entrada de amenazas en el Rectorado de la UNCA, identificando las áreas más vulnerables dentro de los procesos administrativos y educativos.
2. Conocer el riesgo de la seguridad de la información, para poder establecer una base sólida en la construcción de las políticas de seguridad que sean efectivas y adecuadas a las necesidades de la universidad.
3. Identificar los componentes y recursos gestores de Tecnologías de la Información que están involucrados en la protección y gestión de los sistemas de información de la institución.
4. Presentar un manual de políticas de seguridad de la información, desarrollado a partir de los hallazgos obtenidos en los objetivos anteriores, que sirva como herramienta práctica para implementar las medidas de seguridad propuestas.

Este estudio busca establecer un modelo de seguridad que no solo proteja la información institucional, sino que también refuerce la confianza de la comunidad universitaria en el manejo

de los datos y facilite el desarrollo de procesos administrativos y académicos eficientes. Para ello, se tomarán en cuenta marcos normativos internacionales, como la norma ISO 27001, así como los lineamientos del Plan Nacional de Ciberseguridad de Paraguay, para adaptar las políticas de seguridad a las características particulares de la UNCA.

La implementación de un modelo robusto de seguridad de la información no solo es fundamental para proteger los activos digitales de la universidad, sino también para garantizar la continuidad de sus operaciones y promover un entorno académico y administrativo seguro, confiable y transparente. De este modo, el trabajo contribuirá a fortalecer la infraestructura tecnológica de la institución y a fomentar una cultura de ciberseguridad, beneficiando a toda la comunidad universitaria.

El trabajo se alinea con la línea de investigación de Ingeniería Informática, específicamente en el área de Tecnologías para la Información y la Comunicación (TIC). Esto se debe a que el estudio aborda temas fundamentales en la seguridad de la información, la protección de datos y la ciberseguridad dentro de una institución educativa, lo cual es parte esencial de las TIC. La investigación se enfoca en identificar vulnerabilidades, mejorar las prácticas de seguridad, y proponer políticas que optimicen la gestión de la información y la infraestructura tecnológica. Estos elementos son inherentes a las TIC, que abordan el desarrollo, manejo y protección de sistemas de información, con el fin de asegurar la confidencialidad, integridad y disponibilidad de los datos en entornos digitales.

El trabajo se alinea con los siguientes Objetivos de Desarrollo Sostenible (ODS) de la ONU:

1. ODS 4: Educación de Calidad
   Este trabajo promueve un entorno seguro para la información en una institución educativa, lo cual es fundamental para garantizar la continuidad y calidad de los procesos académicos y administrativos. La implementación de políticas de ciberseguridad en el rectorado contribuye a proteger los recursos y datos educativos, permitiendo que la universidad ofrezca una educación de calidad en un entorno seguro y confiable.

2. ODS 9: Industria, Innovación e Infraestructura
   Al mejorar la infraestructura tecnológica y aplicar buenas prácticas de seguridad de la información, el trabajo apoya la construcción de infraestructuras resilientes y sostenibles. Además, promueve la innovación en el ámbito de la educación, asegurando que los sistemas de información sean robustos y estén alineados con los estándares modernos de ciberseguridad, necesarios para enfrentar los desafíos tecnológicos actuales.

3. ODS 16: Paz, Justicia e Instituciones Sólidas
   Este trabajo fomenta la transparencia y la protección de la información en la universidad, lo cual es clave para construir instituciones justas y sólidas. Al mejorar la seguridad de la información, se fortalecen los mecanismos de confianza y se protege la integridad de los datos, contribuyendo a la construcción de instituciones educativas confiables y responsables en el ámbito digital.

Estos ODS están relacionados con la protección de los sistemas de información y la gestión segura de los datos, factores cruciales en un mundo cada vez más digitalizado.

METODOLOGÍA

Tipo de Estudio

El presente trabajo se enmarca en una investigación de tipo descriptiva y analítica, enfocada en el análisis del estado actual de la seguridad de la información en el Rectorado de la Universidad Nacional del Caaguazú y en la formulación de políticas de seguridad basadas en el Plan Nacional de Ciberseguridad. Esta investigación se apoya en un enfoque cuantitativo-cualitativo (mixto) para permitir un análisis profundo de los datos recolectados y su interpretación. Los datos cuantitativos ayudan a obtener mediciones específicas sobre la percepción y conocimiento del personal en torno a las prácticas de seguridad, mientras que los datos cualitativos se enfocan en las percepciones y experiencias relacionadas con las amenazas informáticas.

Población y Muestra

La población del estudio está conformada por el personal administrativo y académico, así como por los estudiantes de la Universidad Nacional del Caaguazú que interactúan con los sistemas de información del rectorado. Se empleó un muestreo no probabilístico por conveniencia, seleccionando una muestra de 50 individuos, entre personal administrativo, docentes y estudiantes, quienes participaron voluntariamente en el estudio.

Variables

Las variables analizadas incluyen: (1) Conocimiento sobre ciberseguridad, (2) Frecuencia de actualización de contraseñas, (3) Aplicación de políticas de seguridad, (4) Percepción de los riesgos de seguridad en la institución, y (5) Uso de herramientas y protocolos de protección (como firewall, antivirus, y cifrado de datos).

Técnicas e Instrumentos de Recolección de Datos

Se utilizaron tres principales técnicas de recolección de datos: (1) observación directa, (2) cuestionarios semiestructurados y (3) entrevistas. La observación directa permitió evaluar las condiciones físicas y tecnológicas de los sistemas de información del rectorado, mientras que los cuestionarios semiestructurados recolectaron información sobre las prácticas de seguridad y conocimientos básicos en ciberseguridad entre los participantes. Las entrevistas se realizaron a

personal clave del área de Tecnologías de la Información y a directivos, quienes aportaron información sobre políticas internas y los recursos destinados a la seguridad de la información.

Procedimiento

1. Fase de Preparación: En esta etapa inicial se diseñaron y validaron los instrumentos de recolección de datos, asegurando que las preguntas de los cuestionarios y entrevistas fueran pertinentes y alineadas con los objetivos del estudio.

2. Recolección de Datos: Se implementaron encuestas y entrevistas presenciales y en línea, asegurando la participación voluntaria y anónima de los encuestados. En paralelo, se realizó la observación de las prácticas y recursos tecnológicos disponibles en el rectorado para identificar posibles vulnerabilidades y deficiencias en los sistemas.

3. Análisis de Datos: Los datos cuantitativos obtenidos de los cuestionarios fueron procesados mediante herramientas estadísticas para obtener frecuencias y porcentajes que permitieran interpretar las prácticas de seguridad de la información. Los datos cualitativos, derivados de entrevistas y observaciones, fueron codificados y categorizados para identificar patrones y tendencias en la percepción de la seguridad y en las prácticas aplicadas.

4. Desarrollo de Propuestas de Mejora: A partir de los resultados obtenidos, se formuló un conjunto de políticas de seguridad alineadas con el Plan Nacional de Ciberseguridad, que sirvan de guía para el rectorado en la implementación de prácticas de seguridad integrales y efectivas.

Consideraciones Éticas

Para la realización de este estudio, se obtuvo el consentimiento informado de todos los participantes, quienes fueron informados de que su participación era voluntaria y que los datos recolectados se utilizarían exclusivamente para fines académicos. Se garantizó la confidencialidad de la información mediante la anonimización de los datos recolectados y el uso de identificadores numéricos. Los resultados y datos individuales no serán divulgados sin la autorización previa de los sujetos de estudio, y el acceso a los mismos quedó restringido al equipo investigador. La investigación fue realizada siguiendo las pautas éticas establecidas por el Comité de Ética de Investigación de la Universidad.

RESULTADOS Y ANÁLISIS

El presente capítulo expone los resultados obtenidos en la investigación realizada en el Rectorado de la Universidad Nacional del Caaguazú, destacando las principales observaciones en cuanto al estado de la seguridad de la información. A través del análisis de datos cuantitativos y cualitativos, se exploran las fortalezas y debilidades en el uso de herramientas de protección, el conocimiento sobre ciberseguridad, la frecuencia de actualización de contraseñas, y la aplicación de políticas de seguridad, entre otros aspectos relevantes. Además, se comparan los hallazgos con estudios previos en el ámbito de seguridad en instituciones educativas, evaluando las áreas críticas que requieren mejoras. Este capítulo pretende proporcionar una perspectiva clara y detallada de la situación actual, señalando las áreas de oportunidad para reforzar la seguridad de la información en el rectorado.

Conocimiento sobre Ciberseguridad

Un aspecto crítico identificado es el nivel de conocimiento del personal sobre prácticas de ciberseguridad. Los resultados revelan que la mayoría de los participantes, un 70%, tienen un conocimiento limitado o nulo sobre estas prácticas, mientras que solo un 30% aseguró poseer conocimientos básicos en el tema. Esto muestra una marcada carencia en la comprensión de principios fundamentales para la protección de los sistemas de información, lo cual podría estar relacionado con la falta de capacitación formal en el área. La ausencia de conocimientos sólidos en ciberseguridad entre el personal expone a la institución a riesgos significativos, ya que los errores humanos y la falta de preparación frente a amenazas cibernéticas suelen ser factores críticos en incidentes de seguridad.

Frecuencia de Actualización de Contraseñas

En relación con la frecuencia de actualización de contraseñas, los resultados muestran que un 81% de los encuestados no realiza cambios periódicos en sus contraseñas, mientras que solo un 19% informó actualizarlas regularmente, al menos cada 30 días. Este dato subraya la falta de adherencia a prácticas recomendadas para mantener la seguridad de acceso a los sistemas de información. La actualización regular de contraseñas es una medida esencial en la protección de los datos, ya que permite minimizar el riesgo de accesos no autorizados. La falta de conciencia sobre esta medida preventiva, aunada a la falta de políticas que promuevan esta práctica, incrementa las vulnerabilidades del sistema institucional.

Aplicación de Políticas de Seguridad

Otro hallazgo relevante es la falta de políticas de seguridad formalmente establecidas en la institución. El 95% de los participantes indicó que no existen políticas específicas que regulen la

seguridad de la información, mientras que solo un 5% reconoció la existencia de políticas parciales, aplicadas únicamente en áreas específicas como el uso de redes internas. La ausencia de políticas de seguridad representa un riesgo importante, pues sin normas claras y procedimientos establecidos, la protección de los datos depende en gran medida de las prácticas individuales de los usuarios. Esto deja abierta la posibilidad de inconsistencias y fallos en la aplicación de medidas de seguridad adecuadas, lo cual expone a la institución a ataques y brechas de seguridad.

Percepción de los Riesgos de Seguridad en la Institución

En cuanto a la percepción de los riesgos de seguridad, los participantes identificaron los mensajes no solicitados (spam) como el riesgo más frecuente, señalado por un 45% de los encuestados. Además, el 27% mencionó las estafas en línea, mientras que el 22% identificó el malware como una amenaza significativa. Estos resultados reflejan una percepción relativamente adecuada de los riesgos que pueden afectar la seguridad de los sistemas, lo cual indica que existe cierta conciencia sobre las amenazas externas. Sin embargo, esta percepción no se traduce en acciones preventivas efectivas, debido a la falta de políticas de seguridad y la carencia de un programa de capacitación enfocado en la identificación y mitigación de riesgos.

Uso de Herramientas de Protección

El análisis de la infraestructura de protección reveló deficiencias significativas. Se observó que el 63% de los dispositivos utilizados en el rectorado carecen de firewall o antivirus actualizado, lo que implica una protección insuficiente contra ataques externos. Adicionalmente, un 50% de los usuarios no utiliza cifrado para proteger datos sensibles, lo cual representa un riesgo en caso de que se produzca un acceso no autorizado a los sistemas. La falta de medidas preventivas adecuadas, como el uso de firewalls, antivirus y cifrado, expone a la institución a posibles ataques, como el robo de información y la infección por malware. Esto también resalta la necesidad de un programa de capacitación que eduque al personal sobre la importancia de estas herramientas y cómo aplicarlas correctamente en el contexto institucional.

Vulnerabilidades y Problemas en la Infraestructura

En el análisis de la infraestructura tecnológica, se detectaron varios problemas críticos. Un alto porcentaje de los sistemas operativos utilizados, alrededor del 78%, no cuenta con licencias vigentes, lo que no solo viola normativas legales, sino que también afecta el rendimiento de los equipos, generando problemas de lentitud y fallos frecuentes. Estos problemas limitan la productividad del personal y aumentan la posibilidad de fallos de seguridad en el sistema. Además, se observó que la instalación de los equipos y el cableado no cumple con los estándares de seguridad ISO, lo cual incrementa el riesgo de incidentes y compromete la seguridad del sistema en su conjunto. Este desorden en la infraestructura no solo afecta el rendimiento de los equipos, sino que también puede facilitar el acceso físico no autorizado a componentes críticos de la red.

Análisis Comparativo con la Bibliografía

Al comparar estos hallazgos con estudios previos, se observa una tendencia similar en instituciones educativas de otros países. Torres-Berrio (2012), por ejemplo, destaca que muchas universidades enfrentan problemas de ciberseguridad debido a la falta de políticas formales y a la dependencia de prácticas individuales para proteger los datos. En la Universidad Nacional del Caaguazú, esta situación parece repetirse, ya que no se cuenta con un marco regulatorio sólido para la protección de la información, lo cual expone a la institución a riesgos semejantes. Al igual que en el estudio de Torres-Berrio, los resultados de este trabajo indican que la falta de capacitación y de políticas específicas en ciberseguridad contribuyen a la vulnerabilidad de las instituciones académicas frente a amenazas externas y errores internos.

Fortalezas y Limitaciones del Estudio

Una de las fortalezas de este estudio radica en la identificación precisa de las deficiencias que enfrenta la institución, lo que proporciona una base sólida para el desarrollo de políticas de seguridad de la información. Esta investigación permite establecer un diagnóstico claro que servirá como punto de partida para la implementación de un plan integral de seguridad en el rectorado. Sin embargo, una limitación importante es el tamaño de la muestra utilizada, que podría limitar la representatividad de los resultados y su generalización a toda la población del rectorado. Además, el diseño de estudio transversal impide analizar cambios en el tiempo, lo cual sería necesario para evaluar la efectividad de las políticas de seguridad a largo plazo.

Perspectivas Futuras

A partir de los resultados obtenidos, se sugieren varias líneas de acción para mejorar la seguridad de la información en el Rectorado de la Universidad Nacional del Caaguazú. En primer lugar, es esencial implementar un programa de capacitación en ciberseguridad dirigido a todo el personal, con el objetivo de elevar su nivel de conocimiento y reducir el riesgo de incidentes relacionados con errores humanos. Asimismo, es fundamental desarrollar e implementar un conjunto de políticas de seguridad que regulen el uso de herramientas de protección, la actualización de contraseñas, y el acceso a sistemas y datos sensibles. Estas políticas deben estar alineadas con el Plan Nacional de Ciberseguridad y otros estándares internacionales como ISO 27001.

Futuras investigaciones podrían enfocarse en el monitoreo y evaluación del impacto de estas políticas y programas de capacitación mediante estudios longitudinales que permitan observar los cambios y mejoras a lo largo del tiempo. Adicionalmente, se recomienda estudiar la implementación de nuevas tecnologías y protocolos de seguridad, como la autenticación

multifactor y el cifrado avanzado, que contribuyan a reducir los riesgos de ciberseguridad en entornos educativos.

Este capítulo de Resultados y Análisis revela un panorama amplio y detallado de la situación actual de la seguridad de la información en la Universidad Nacional del Caaguazú, destacando tanto las fortalezas como las debilidades encontradas en el sistema. A partir de estos hallazgos, es posible proponer medidas específicas que permitan a la institución mejorar su infraestructura de seguridad y adoptar una cultura organizacional orientada a la protección de sus recursos informáticos y la integridad de sus datos.

CONCLUSIONES Y RECOMENDACIONES

Este capítulo presenta las conclusiones derivadas de la investigación y proporciona recomendaciones concretas para fortalecer la seguridad de la información en el Rectorado de la Universidad Nacional del Caaguazú. Los hallazgos han puesto en evidencia las áreas críticas que necesitan atención inmediata, desde la falta de capacitación en ciberseguridad hasta las deficiencias en la infraestructura y la ausencia de políticas formales. Con estas conclusiones y recomendaciones, se espera contribuir a la creación de un entorno seguro para los sistemas de información en la institución.

Conclusiones

La investigación realizada permite llegar a las siguientes conclusiones, cada una alineada con los objetivos y preguntas planteadas al inicio del estudio:

1. Necesidad de Capacitación en Ciberseguridad

La investigación muestra que una de las principales vulnerabilidades en la seguridad de la información en el rectorado es la falta de conocimientos en ciberseguridad entre el personal administrativo, académico y estudiantil. El 70% de los participantes manifestó desconocer prácticas básicas de protección de la información, lo que refleja la ausencia de formación en este ámbito. Esta carencia expone a la institución a riesgos como errores humanos y el desconocimiento de amenazas comunes, lo cual hace que el personal no esté preparado para identificar y mitigar posibles incidentes de seguridad.

2. Ausencia de Políticas Formales de Seguridad

Un 95% de los encuestados indicó que el rectorado carece de políticas de seguridad de la información, lo cual permite prácticas informales e inconsistentes en el uso y manejo de los sistemas de información. La falta de normas y procedimientos claros debilita la protección de los datos y permite la existencia de riesgos innecesarios. Sin una estructura formal de políticas, la seguridad depende de las decisiones individuales de cada usuario, lo que aumenta la probabilidad de errores y vulneraciones.

3. Deficiencias en la Infraestructura Tecnológica

La infraestructura tecnológica del rectorado presenta varias deficiencias, como el uso de sistemas operativos sin licencias válidas en aproximadamente el 78% de los equipos. Esto no solo implica incumplimientos legales, sino que afecta el rendimiento de los sistemas y aumenta el riesgo de fallos de seguridad. Además, el desorden en la instalación y el cableado de los equipos, que no cumple con los estándares ISO, incrementa los riesgos de fallos técnicos y de seguridad. Estas condiciones no solo limitan la productividad, sino que facilitan accesos no autorizados y exponen los sistemas a posibles ataques.

4. Insuficiente Frecuencia en la Actualización de Contraseñas y Uso de Herramientas de Protección

Un hallazgo importante es la baja frecuencia en la actualización de contraseñas y el uso limitado de herramientas de protección, como firewalls y cifrado. El 81% de los usuarios no realiza cambios regulares en sus contraseñas y el 63% de los dispositivos no cuenta con antivirus o firewall actualizado. Esto facilita el acceso no autorizado a los sistemas y compromete la confidencialidad y la integridad de la información. La baja frecuencia en la actualización de contraseñas y la ausencia de prácticas básicas de seguridad suponen una brecha crítica en la protección de los datos.

5. Percepción Limitada de los Riesgos de Seguridad

Si bien los usuarios identificaron algunos riesgos, como mensajes no solicitados y malware, la falta de políticas de seguridad y programas de capacitación dificulta que esta percepción se traduzca en acciones preventivas efectivas. La ausencia de una cultura de ciberseguridad en la institución refuerza la idea de que los usuarios no están plenamente conscientes de la importancia de la seguridad de la información en su trabajo diario, lo cual limita la efectividad de cualquier medida de seguridad que se implemente.

Recomendaciones

Con base en las conclusiones anteriores, se presentan las siguientes recomendaciones para mejorar la seguridad de la información en el Rectorado de la Universidad Nacional del Caaguazú. Estas acciones están orientadas a establecer prácticas de seguridad sostenibles y eficaces que respondan a las necesidades específicas de la institución.

1. Implementación de un Programa de Capacitación en Ciberseguridad

La creación de un programa de capacitación permanente en ciberseguridad para todo el personal y estudiantes es una prioridad. Este programa debería incluir talleres y capacitaciones regulares sobre temas fundamentales, como manejo seguro de contraseñas, identificación de amenazas comunes, y uso adecuado de herramientas de protección como antivirus y firewalls. Un programa bien estructurado permitiría reducir la incidencia de errores humanos, fomentar una cultura de seguridad y preparar al personal para actuar con rapidez y efectividad ante posibles incidentes.

2. Desarrollo y Aplicación de Políticas de Seguridad de la Información

La formalización de un conjunto de políticas de seguridad de la información es esencial para la institución. Estas políticas deben regular aspectos clave como el acceso a la información, el uso de contraseñas, el manejo de datos sensibles y la gestión de incidentes de seguridad. Las políticas deben diseñarse con base en el Plan Nacional de Ciberseguridad y en estándares internacionales como ISO 27001, y se deben comunicar de manera clara y efectiva a todos los miembros de la comunidad universitaria. La implementación de estas políticas reducirá la dependencia de prácticas informales y garantizará un marco de seguridad coherente y sostenible.

3. Actualización y Optimización de la Infraestructura Tecnológica

Se recomienda que el rectorado actualice los sistemas operativos en uso, asegurando que todos los equipos cuenten con licencias válidas y actualizaciones de seguridad periódicas. Además, se debe reorganizar la instalación de los equipos y cableado de acuerdo con los estándares

internacionales de seguridad, como los que se establecen en las normativas ISO. Estas acciones no solo contribuirán a mejorar el rendimiento de los sistemas, sino que también reducirán las posibilidades de fallos técnicos y accesos no autorizados, optimizando así el entorno tecnológico de la institución.

4. Implementación de Herramientas de Protección y Mantenimiento de Esta

Para reducir el riesgo de accesos no autorizados y asegurar la integridad de la información, se recomienda que todos los dispositivos y redes del rectorado cuenten con sistemas de firewall, antivirus y cifrado de datos actualizados. Además, es importante promover el uso de autenticación multifactor para los accesos más críticos y fomentar la actualización periódica de contraseñas. Estas medidas protegerán de forma integral los sistemas de información y reducirán las vulnerabilidades ante amenazas externas.

5. Fomento de una Cultura de Ciberseguridad en la Institución

La institución debe promover la importancia de la ciberseguridad a través de campañas informativas, material educativo y talleres que refuercen el compromiso de todos los miembros de la comunidad universitaria. La creación de una cultura de ciberseguridad permite que el personal y los estudiantes comprendan la relevancia de sus prácticas en el manejo de la información y adopten una postura activa en la protección de los datos y sistemas institucionales.

Propuesta de Acción

Para asegurar la implementación de estas recomendaciones y fomentar una gestión proactiva de la seguridad de la información, se propone la creación de un Comité de Ciberseguridad en el rectorado. Este comité debe estar compuesto por representantes de las áreas de Tecnologías de la Información, administración, cuerpo docente y estudiantil, quienes trabajen en conjunto para supervisar la implementación de políticas de seguridad, coordinar actividades de capacitación y realizar auditorías periódicas para evaluar la efectividad de las medidas de seguridad. El comité también deberá realizar un seguimiento constante de las amenazas emergentes y proponer mejoras a las políticas y prácticas de seguridad según sea necesario.

El comité también podría liderar la elaboración de un manual de ciberseguridad específico para la universidad, el cual incluya lineamientos detallados y procedimientos de acción en caso de incidentes. Este manual serviría como guía práctica para todo el personal y estudiantes, facilitando la adopción de las políticas y procedimientos recomendados. Además, el comité debería desarrollar un sistema de monitoreo y alerta que permita la detección temprana de amenazas y fallos en la infraestructura, asegurando así una respuesta rápida y eficaz ante posibles incidentes.

Conclusión Final

La investigación realizada ha puesto en evidencia la necesidad urgente de implementar medidas de seguridad de la información en el Rectorado de la Universidad Nacional del Caaguazú. La adopción de las recomendaciones y la creación de un comité de ciberseguridad contribuirán

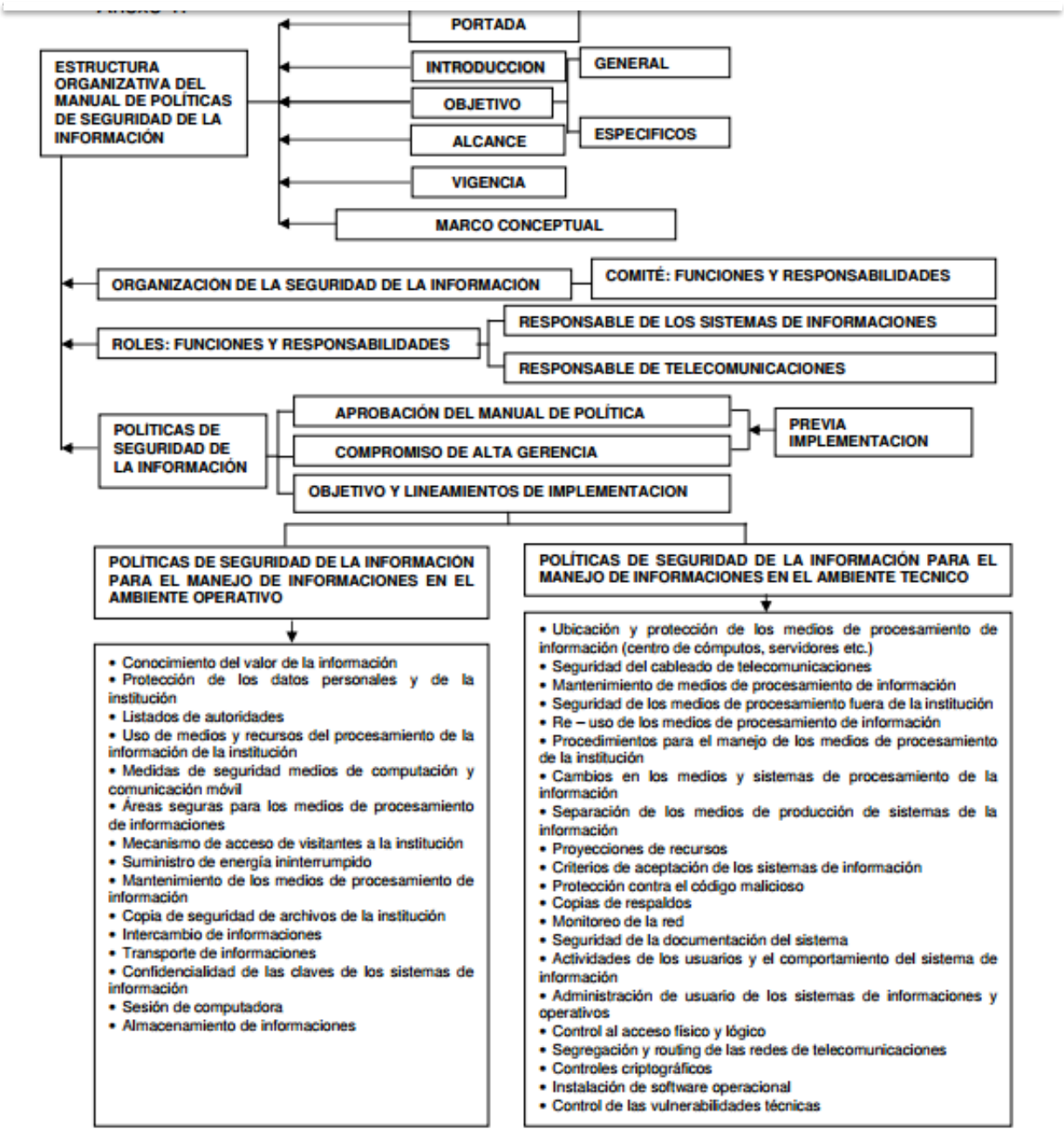
significativamente a mejorar la protección de los datos y recursos informáticos de la institución. Con un enfoque integral, que incluya capacitación continua, políticas formales, mejoras en la infraestructura y la promoción de una cultura de ciberseguridad, el rectorado puede construir un entorno de trabajo más seguro y confiable, alineado con los estándares nacionales e internacionales de seguridad de la información.

BIBLIOGRAFÍA

- Torres-Berrios, L. (2012). Amenazas a la seguridad de la información computadorizada en las universidades en Puerto Rico desde la perspectiva de los profesionales del área desistemas de información.
- Secretaria nacional de tecnologías de la información y comunicación (2013) Plan nacional de ciberseguridad, Gobierno Nacional. Paraguay.
- Soriano, Miguel (2014) *Seguridad en redes y seguridad de la información*, Facultad de electrotecnia, Praga
- Revista INEM (2013) *técnicas de seguridad con la normativa ISO 27002*, 1ºedic, Ecuador
- Voutssas, Juan (2010) *preservacion documental digital y seguridad informatica.*UNAM,Mexico,recuperado:http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008
- Dussan, Ciro (2006*) Políticas de seguridad informatica*,Red de revistas cientificas de america latina. recuperado: http://www.redalyc.org/html/2654/265420388008/
- Alvarado, L. (2011). Diseño de un Plan de Gestión de Seguridad de la Información.
- Borbón, J. (2011) "Buenas prácticas, estándares y normas". REVISTA SEGURIDAD, DEFENSA DIGITAL.
- Aguilera, P. (2010). "Seguridad informática. Informática y comunicaciones". Editorial Editex, S. A.
- Mifsud, E. (2012). "Políticas de seguridad. ¿Cómo podemos proteger el sistema informático?".
- Segunda Cohorte del Doctorado en Seguridad Estratégica. (2014). "Seguridad de la Información".
- Téllez, J. (1988). Contratos, riesgos y seguros informáticos. Universidad Autónoma de México. UNAM.
- TECNOLOGÍAS DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - CÓDIGO DE PRÁCTICA PARA LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN (ISO/IEC 27002:2013 + Cor 1:2014 + Cor 2: 2015, IDT)
- SENATICs. (2017, marzo). Retos, roles y compromisos. Plan Nacional de Ciberseguridad, 46.

ANEXOS

Estructura del manual de políticas de seguridad de la información para el Rectorado de la Universidad Nacional de Caaguazú.



Nombre del encuestador: _____ Nº de encuestador:____

Nombre del encuestado: _____ Nº de encuesta:_____

Hora de comienzo: __ : __ Hora de finalización: __ : __

Presentación del encuestador

Sr. / a

Solicito su colaboración. Responda el siguiente cuestionario que tiene el propósito de conocer su opinión respecto al tema **"Políticas de Seguridad en Sistemas de Información para el rectorado de la Universidad Nacional del Caaguazú"**. Y nos gustaría saber sus conocimientos sobre seguridad de información.

Agradezco su colaboración.

Responsable: Justino Rodrigo Rojas Sartorio.

A. Responde los siguientes planteamientos

1. ¿Qué entiendes por las Tecnologías de información y comunicación?

2. ¿Qué la seguridad de la información?

3. ¿Cuáles son los probables riesgos que puede tener la seguridad de la información?

4. ¿Qué entiendes sobre confidencialidad de la información?

5. ¿Qué Clase de información maneja frecuentemente?

- Impresa o escrita a mano
- Grabada con asistencia técnica
- Transmitida por correo electrónico
- Incluida en sitios web
- Mostrada en video conferencias
- Redes sociales

6. ¿Se aplican políticas de seguridad en la institución?

- Si
- No

7. Cuál es la frecuencia de renovación de su contraseña en la protección de sus datos

8. ¿Posee capacitación con respeto a riesgos de seguridad?

- Si
- No

9. ¿Cuáles son las áreas que se necesitan mayor control de riesgos de seguridad?

- Redes
- Correo electrónico
- Infraestructura

10. ¿Conoce las políticas de uso de internet?

- Si
- No

11. ¿Conoce el uso adecuado de los sistemas de correo electrónico?

- Si
- No

12. Hay restricciones en el acceso a los programas y archivos?

- Nada
- Muy poco
- Mucho

13. Hay medidas alternativas de contingencia para la transmisión de información?

- Si ,¿ Cuales son?
- No

14. ¿Cuál es el horario promedio de los usos de los sistemas de información?

- De 7:00 a 15:00
- De 15:00 a 22:00

15. ¿Se dispone de un plan documentado en la que constan la normativas de seguridad de la información?

- Si
- No

B. Marque con una X la puntuación que considere correcta (1 nunca, 5 siempre)

Fallas de la seguridad	1	2	3	4	5
Manipulación de aplicaciones de software					
Accesos no autorizados a la web					
Virus					
Perdida, fuga de información					
Ataques de aplicaciones web					
Infección de Malware					
Robo de información					
Acceso indebido					

Mecanismos de protección	1	2	3	4	5
Smart Cards					
Antivirus					
Contraseñas					
Cifrando datos					
Firewall Hardware					
Firewall Software					
VPN/ IP sec					
Proxies					
Sistema de detección de intrusos					
Administración de logs					
ADS (Anomaly detected Systems)					
Firewall de base de datos					
Tercerización de la seguridad de la información					
Otros (Herramientas scanning)					