TRABAJO DE GRADO
Opción Seminario.

"ALCALDÍA MUNICIPAL DE VILLA NUEVO SOL"

Corporación Universitaria Remington.
Facultad de Ingenierías
Ingeniería de Sistemas

Yamir Palacios Orejuela

Jorge Leonardo Ramírez Restrepo - docente del seminario.
Seminario
2026

Tabla de Contenidos

Resumen

Este informe técnico analiza el caso "**ALCALDIA MUNICIPAL VILLA NUEVO SOL**", enfocado en una situación de ciberseguridad, y este tiene como propósito identificar los principales activos, amenazas, vulnerabilidades y riesgos que esta puede llegar a afectar la información de la organización así mismo la continuidad de sus actividades, A partir de este caso de estudio se realizará una análisis sobre la organización basada en conceptos y buenas prácticas vistas en el seminario de ciberseguridad organizacional, teniendo como base principal las normas que se aplicaran.

Este caso de estudio se realiza un análisis de la situación actual de la alcaldía, notando que los principales activos, amenazas y vulnerabilidades que se encuentran expuestas así como los riesgos que pueden afectar el desarrollo normal de las actividades. Para este análisis se toma como base los conceptos vistos durante el seminario de ciberseguridad organizacional y las diferentes normas, estándares y las buenas prácticas que relacionan la seguridad de la información y la gestión de los riesgos.

Con base al análisis realizado, se presentan las políticas de seguridad, controles administrativos, técnicos y físicos y así como recomendaciones para poder mejorar la protección de los activos y así fortalecer la respuesta oportuna ante problemas ocasionados y mantener las operaciones funcionales en la alcaldía, al final este informe busca presentar una propuesta para mejora que pueda apoyar a tomar decisiones que ayuden a mejorar y mantener una cultura organizacional que se puede enfocar en la protección de la información y la gestión adecuada de la ciberseguridad

Palabras clave

- **Ciberseguridad Organizacional**
- **Seguridad de la información**
- **Activos**
- **Gestión de riesgos**
- **Continuidad del negocio**

Marco conceptual y normativo

Conceptos fundamentales de ciberseguridad

La ciberseguridad es una mezcla de políticas, tecnología y buenas prácticas que buscan proteger información sensible, sistemas informáticos, redes y servicios digitales ya que hay amenazas que pueden afectar su funcionamiento, esta busca reducir la mayor cantidad de riesgos que puedan originar estos casos y así garantizar que las organizaciones desarrollen su papel como debe de ser (National Institute Of Standards And Technology [NIST],2024)

Actualmente muchas organizaciones dependen cada vez más de la tecnología de la información para lograr algunos objetivos, Por este motivo, la seguridad de la información se ha convertido en un aspecto fundamental para que sus procesos no paren, proteger los datos y generar más confianza con los usuario y entidades. La seguridad de la información busca salvaguardar durante todo el tiempo que la entidad lo requiera o exista así se evitan perdidas, alteraciones o accesos no autorizados. (ISO, 2022).

El aplicar estos principios permite que se fortalezca la gestión de manejo de la información y así reducir la gran posibilidad de algún fallo o incidente de seguridad que puedan afectar la operación de una organización. En las entidades públicas como en este caso “ALCALDIA MUNICIPAL DE VILLA NUEVO SOL”, donde la información se administra y se almacena ya que esta es de ciudadanos, contratistas, servidores públicos y procesos administrativo, esto nos obliga a tener buenas prácticas de ciberseguridad y resulta que es fundamental para proteger los activos de información, garantiza la información y la continuidad de los servicios prestados y fortalecer la confianza de la ciudadanía en la gestión institucional.

La ciberseguridad está estrechamente relacionada con la seguridad de la información ya que esta se enfoca en proteger los recursos más importantes para mucha o todas las organizaciones que es la información, según la norma o estándar ISO/IEC 27001:2022 la seguridad de la información busca mantener la confidencialidad, la integridad y la disponibilidad de los datos durante todo el tiempo de vida y permitiendo que únicamente las personas autorizadas puedan acceder a ella y que la información no sea modificada sin autorización y que permanezcan disponible cuando se necesite para que se desarrollen las actividades necesarias en la alcaldía

Los principios son conocidos como la triada CIA, ya que la confidencialidad garantiza que la información solo sea conocida por las personas o entidades autorizadas, la integridad busca que la información mantenga intacta sin ser modificados por personas que no tienen acceso a ella y la disponibilidad nos ayuda q a que la información debe de estar en el tiempo oportuno para su uso y desarrollar las actividades necesarias.

Marco normativo

El análisis de la ciberseguridad en la Alcaldía Municipal de Villa Nuevo Sol se necesita considerar el marco legal colombiano y los estándares internacionales para la protección de la información y gestionar mejor la seguridad en la institución pública, debido que la entidad tiene datos de los ciudadanos, financiera y además presta el servicio digital a la comunidad, resulta necesario identificar las normas y estándares que esta debe de seguir para proteger o salvaguardar la información anteriormente mencionada y de esta manera aplicar buenas prácticas de seguridad de la información.

Las normas y estándares internacionales presentados a continuación las seleccione por su relación con la situación identificadas en el diagnóstico del caso presentado como el tratamiento de los datos personales, el uso de credenciales compartidos, ausencia de políticas de seguridad y la gestión de los riesgos que esta puede presentar. Su aplicación contribuye al fortalecimiento de la protección de la información y el complimiento de las normas vigentes y que esto sea una mejora continua de la seguridad de la información en la organización

Tabla 1. Normatividad aplicable.

Norma o estándar	***Propósito***	***Aplicabilidad en la organización***

Ley 1581 de 2012	Deja claro las disposiciones generales para la protección de los datos personales y esta garantiza el derecho de las personas a conocer, actualizar y modificar la información que sea almacenadas de ellos.	Esta ley aplica en la alcaldía porque administra los datos de los ciudadanos, funcionarios, contratistas y algunos o todos los proveedores, ya que se enfoca en el tratamiento y protección adecuada del derecho a la privacidad
Ley 1273 de 2009	Esta modifica el código penal de Colombia e ingresa los delitos informáticos y establece sanciones a quienes intente robar información de sistemas informáticos	Esta ley permite proteger jurídicamente la información de una institución frente a accesos no autorizado, alteraciones de datos o info, fraude y otros delitos informáticos que pueden afectar el funcionamiento de la alcaldía
ISO 27001	Tiene establecido los requisitos para implementar un sistema de gestión de seguridad de la información y esta contempla la mejora continua y la gestión de riesgos.	Se toma como guía para establecer las políticas, procedimientos y los controles que permiten proteger la información de la alcaldía y así poder fortalecer la seguridad.
ISO 27005	Nos da indicaciones para poder identificar, analizar y evaluar los riesgos y tratar de relacionarlos con la seguridad de la información.	Nos ayuda a identificar las amenazas, vulnerabilidades y riesgos que presenta la alcaldía y así priorizar formas de mantener el control y tomar las mejores decisiones para reducir riesgos por perdida de datos o información
ENISA	Publica algunas recomendaciones, maneras o metodologías para tener	Las directrices de esta sirven como referencia de

	una buena práctica y así fortalecer la ciberseguridad y poder mejorar la capacidad de respuesta ante una amenaza.	incidentes, la cultura de la ciberseguridad y la adopción de buenas prácticas en la alcaldía.

Las normas, estándares y leyes seleccionadas sirven como guía para fortalecer la seguridad de los datos del a alcaldía municipal villa nuevo sol, y las leyes colombianas enmarcan las obligaciones relacionadas con la protección de los datos personales y los delitos informáticos, pero las recomendaciones de ENISA nos da buenas prácticas para la gestión de riesgos y así poder implementar un control de seguridad y proteger los activos de información y esta al ser aplicada de cierta manera nos ayuda a mejorar la gestión de la ciberseguridad, reducir posibles incidentes y ayudar a mantener la alcaldía en funcionamiento (Congreso de Colombia, 2009; Congreso de Colombia, 2012; International Organization for Standardization [ISO], 2018; International Organization for Standardization [ISO], 2022; European Union Agency for Cybersecurity [ENISA], 2023; National Institute of Standards and Technology [NIST], 2024).

Marco contextual

La transformación digital nos ha permitido que las entidades públicas mejoren todos los servicios por medio de la tecnología, sistemas de información y plataformas que agilizan los procesos de los ciudadanos, sin embargo el estar dependiendo de la tecnología también aumenta la exposición a las amenazas que pueden llegar a afectar la seguridad de la información y en funcionamiento de esta organización. El contexto resulta un poco o muy importante conocer las características de la organización, en este caso de estudio y la problemática identificada buscando comprender el entorno en el que se realiza al análisis de ciberseguridad, por eso esta información será posible que sea identificada por medio de los principales activos de la información, los riesgos que existen y algunas de las medidas que ayudarían a fortalecer la protección de la información y la continuidad de los servicios que esta entidad estaría prestando

Descripción de la organización

La alcaldía Municipal Villa Nuevo Sol es una entidad pública encargada de la administración del municipio y de estar prestando el servicio dirigido a la comunidad Villo Nuevo Sol. Su actividad principal consiste en planificar y ejecutar programas, proyectos de manera pública enfocada al desarrollo económico y social del municipio así podrá garantizar que se cumplan las funciones establecidas por la normativa vigente.

La estructura de la organización está conformada por la oficina del alcalde, las secretarias municipales y las diferentes dependencias o ramificaciones de estas, las cuales trabajan de manera conjunta para atender las necesidades de la población del municipio y así poder garantizar el funcionamiento de la administración pública. Recordemos que cada dependencia desarrolla funciones específicas que van relacionada con áreas como hacienda o planeación por ejemplo.

Como apoyo a las actividades de la alcaldía, las organizaciones tienen a la mano recursos tecnológicos como computadores, servidores, redes de comunicación, base de datos, sistemas de información ciudadana (Plataforma de radicado) y demás… los cuales permiten almacenar, procesar y compartir la información necesaria para que se den las actividades en esta entidad. Estos recursos son utilizados diariamente por funcionarios y contratistas para poder garantizar la prestación del servicio y lo cual favorece el adecuado funcionamiento de la administración municipal.

La alcaldía hace sus actividades en un entorno donde el uso de la tecnología es cada vez más importante para la gestión pública, por este motivo, la misma debe de mantener un excelente funcionamiento de sus recursos tecnológicos y de sus procesos administrativos que resultan muy fundamental para poder brindar una atención eficiente a la ciudadanía y así poder cumplir con los objetivos de la institución o entidad pública.

Problemática identificada

En el caso de la Alcaldía Municipal Villa Nuevo Sol se identificaron diferentes situaciones que dejan a la vista debilidades en la gestión de la seguridad de la información. Entre ella está la ausencia de políticas de seguridad que claramente nunca fueron definidas, el uso compartido de credenciales, la falta de controles para proteger la información y la gran falta de un proceso estructurado para identificar y poder gestionar los posibles riesgos que están relacionados con los sistemas de información.

Esta situación aumento la gran posibilidad de que la información institucional sea alterada o vista por personal no autorizado y así afectando los procesos internos y los servicios que se prestan a la comunidad Vill Sol, adicional de que al tratarse de una entidad pública que administra información personal de los ciudadanos y documentación que claramente son confidenciales y cualquier incidente o problema de seguridad puede generar consecuencias importantes para la organización y esto afecta la confianza de la ciudadanía.

El desarrollo del presente informe justifica la necesidad de analizar la situación actual alcaldía, además de identificar los activos de información más importantes y poder reconocer las amenazas, vulnerabilidades y posibles riesgos y establecer las bases para agregar controles y políticas que ayuden a fortalecer la seguridad de la información y mejorar la ciberseguridad de la organización

Identificación y análisis de activos

Inventario de activos

Los activos de la información son todos aquellos recursos que tienen un valor para una organización y que ayudan a que se cumplan los objetivos de esta. Estos pueden estar representados por las personas, equipos de sistemas, documentos o la información ya que son importantes para el desarrollo de las actividades de la organización, al saber cuáles son se permite conocer cuales saben de protegerse y cuales son importantes para que se garantice el funcionamiento de los servicios de la organización.

En la Alcaldía municipal Villa Nuevo Sol los activos apoyan el desarrollo de los procesos tanto administrativos, financieros y la atención de la ciudadanía ya que gran parte de la información se organiza mediante herramientas tecnológicas y esto es importante conocer cuáles son los recursos más importantes para la entidad y el nivel de gravedad que estos presentan, así se permite establecer prioridades en su protección y facilitar el análisis que se realizará en los siguientes capítulos del informe.

Tabla 2. Inventario de activos

Activo	***Tipo***	***Descripción***	***Criticidad***

Base de datos de los ciudadanos	Tecnológico	Almacena información personal y de los administradores	Alta
Sistema de información institucional	Tecnológico	Gestiona y realiza los procesos administrativos y la prestación de servicios	Alta
Servidor principal	Físico	Aloja los sistemas y la información institucional	Alta
Funcionarios	Humano	Utilizan la información y los sistemas institucionales	Alta
Computadores	Físico	Son las herramientas usadas para desarrollar las actividades diarias.	Media
Red de comunicación	Tecnológico	Permite que se realice la comunicación entre equipos y sistemas	Alta
Documentación institucional	Información	Expedientes, contratos, actos administrativos y demás documentos oficiales.	Alta

Correo electrónico Institucional	Tecnológico	Medio oficial por el cual se realiza la comunicación interna y externa.	Media

Los activos presentados en la tabla anterior cumplen funciones importantes Dentro de la Alcaldía Municipal Villa Nuevo Sol, ya que permiten desarrollar todas las actividades tanto administrativas como las del servicio a la comunidad, sin embargo algunos tienen un mayor nivel de gravedad porque tienen o cumplen un papel muy importante en la organización.

La base de datos donde esta alojada toda la información tanto ciudadana como administrativo es uno de los activos más importante y esta es usada para la prestación de diferentes servicios, al tener la base datos comprometida puede alterar el funcionamiento tanto de los servicios como a la comunidad Villa Nuevo Sol.

El sistema y el servidor también son considerados muy importantes o de alta importancia porque estos dan acceso a funciones que la organización necesitan para realizar sus actividades diarias y darle solución a la ciudadanía en base a sus necesidades y al verse comprometido, afectaría gravemente los procesos de la entidad.

Los funcionarios desempeñan un papel importante ya que por medio de ellos se da solución a los problemas de los problemas que presenta la comunidad teniendo como base las tecnologías de la tabla y así los usos adecuados de estos recursos depende, en gran medida de sus conocimientos y el cumplimiento de las políticas institucionales.

Identificar estos activos ayuda a que la base y el desarrollo del presente informe permitirá analizar posteriormente posibles amenazas que puedan afectar, así establecer medidas de seguridad más adecuadas.

Análisis de amenazas y vulnerabilidades

Tabla 3. Amenazas y vulnerabilidades

Activo	*Amenaza*	*Vulnerabilidad*
Base de datos de ciudadanos	Acceso no autorizado	Credenciales compartidas
Sistemas de PQRS	Ransomware	Servidores sin actualizar
Correos institucionales	Phishing	Falta de capacitación
Red Institucional	Malware	Ausencia de segmentación y monitoreo
Servidores	Falla tecnológica	Copias de seguridad sin verificar
Funcionario	Ingeniería social	Escasa cultura de ciberseguridad

El análisis de amenazas y vulnerabilidades realizado para la alcaldía municipal villa nuevo sol permitió identificar los principales factores que podrían comprometer la confidencialidad y la disponibilidad de la información institucional, la relación entre los activos de información y las amenazas facilita comprender como una debilidad existe y puede ser aprovechada para que una entidad o institución se quede sin funcionar y la prestación de los servicios públicos

Unos de los riesgos más importantes van con la base de datos donde esta almacenado toda la información de los ciudadanos y los procesos administrativos, la amenaza de acceso no autorizado combinada con la vulnerabilidad enlazada con el mal uso de compartir las credenciales, esto incrementa significativamente la posibilidad de que las personas no autorizadas consulten, modifiquen o eliminen información sensibles y esta situación podría generar incumplimiento a la ley 1581 de 2012 sobre la protección de los datos personales y esto afecta la confianza de la ciudadanía y ocasionar sanciones para la entidad por no estandarizar aquella ley.

El sistema PQRS el cual soporta la atención de las peticiones, queja, reclamos y solicitudes presentadas por los ciudadanos al presentar una amenaza de una Ransomware

presenta un riesgo elevado debido a que los servidores pueden presentar vulnerabilidades solo por la falta de actualizaciones de seguridad o parches. En caso de que este suceso se dé la información podría quedar cifrada y el sistema estaría fuera de servicio durante un tiempo considerado, afectando la continuidad de las actividades administrativas y el incumplimiento de los procesos hacia la comunidad.

Los correos administrativos o institucionales conforman otro activo altamente expuesto. El phishing continúa siendo unas amenazas más frecuentes contra la organización. En espacial cuando existe una limitada capacitación al personal para poder identificar este tipo de ataques. Un funcionario que entregue sus credenciales o descargue archivos desde fuentes dudosas podría facilitar el acceso de atacantes a los sistemas comprometiendo la información confidencial y permitiendo la propagación de otros ataques dentro de la infraestructura tecnológica.

La red institucional también presenta una activo de alta importancia, la ausencia de mecanismos adecuados de monitoreo facilita la propagación de malware entre los diferentes equipos conectados a esta red, aumentando el impacto de un incidente de seguridad.
La falta de controles de monitoreo limita la capacidad de detectar actividades sospechosas de manera temprana y dificultando la respuesta a tiempo de parte del área de tecnología o sistemas.

Los servidores institucionales concentran aplicaciones, bases de datos y servicios esenciales para el funcionamiento de la alcaldía. La existencia de copias de seguridad sin verificar constituye una vulnerabilidad importante, ya que, ante una falla tecnológica o un ataque de Ransomware, la organización podría enfrentar dificultades para recuperar la información y restablecer los servicios. Esta situación incrementa el tiempo de recuperación y afecta directamente la disponibilidad de los procesos institucionales. Finalmente, el factor humano representa uno de los elementos más críticos del análisis. La escasa cultura de ciberseguridad favorece la materialización de ataques de ingeniería social, debido a que los funcionarios pueden desconocer las buenas prácticas para el manejo seguro de la información y de los recursos tecnológicos. La ausencia de programas permanentes de sensibilización incrementa la probabilidad de errores humanos que pueden derivar en incidentes de seguridad. Los activos que representan mayor riesgo para la Alcaldía Municipal Villa Nuevo Sol son la base de datos de ciudadanos, los servidores institucionales y el sistema de PQRS, debido a la sensibilidad de la información que administran y a las consecuencias que tendría una interrupción de los servicios. Asimismo, el phishing y la ingeniería social destacan como amenazas prioritarias porque aprovechan vulnerabilidades asociadas al comportamiento de los usuarios. Estos resultados evidencian la necesidad de implementar políticas de seguridad, controles técnicos y programas permanentes de capacitación que permitan reducir la probabilidad de ocurrencia de incidentes y fortalecer la protección de la información institucional.

Análisis y gestión de riesgos

Metodología de análisis

Para la valoración de los riesgos se utilizó una metodología cualitativa, tomando como referencia los lineamientos de la norma ISO/IEC 27005:2022 sobre gestión de riesgos de seguridad de la información. Se evaluaron dos criterios para cada riesgo identificado: el **impacto**, entendido como la magnitud de las consecuencias sobre la confidencialidad, integridad o disponibilidad de la información en caso de materializarse el riesgo; y la **probabilidad**, entendida como la posibilidad de que el riesgo llegue a ocurrir dado el contexto actual de la organización.
Ambos criterios se calificaron en tres niveles (Alto, Medio, Bajo), de acuerdo con los siguientes parámetros:
Impacto

- **Alto:** compromete información sensible o crítica (datos personales, bases tributarias, continuidad de servicios esenciales) o genera incumplimiento normativo.
- **Medio:** afecta procesos institucionales de forma parcial o temporal, sin comprometer directamente información crítica.
- **Bajo:** genera afectaciones menores y de fácil corrección.

Probabilidad

- **Alta:** existe una vulnerabilidad identificada y activa que facilita la ocurrencia del riesgo (ej. credenciales compartidas, servidores sin actualizar).
- **Media:** requiere de una condición adicional (error humano, acceso previo) para materializarse.
- **Baja:** requiere de varias condiciones simultáneas poco probables en el contexto actual.

El nivel final de cada riesgo se obtuvo combinando ambos criterios, priorizando aquellos riesgos clasificados como Alto en al menos una de las dos dimensiones cuando la otra dimensión es igualmente crítica para la operación institucional.

Matriz de riesgos

Tabla 4. Matriz de riesgos

Riesgo	***Impacto***	***Probabilidad***	***Nivel***

Acceso no autorizado a la base de datos de los ciudadanos	Alto	Alta	Alto
Phishing dirigido a funcionarios	Medio	Alta	Alto
Ransomware en servidores institucionales	Alto	Alto	Alto
Modificación de la información de sistema PQRS	Alto	Media	Alto
Fuga de información del por compartir credenciales o información.	Alto	Alto	Alto
Caída de servicios por fallas de infraestructura	Medio	Media	Medio

La matriz de riesgos muestra que los riesgos con mayor prioridad para la Alcaldía Municipal Villa Nuevo Sol son el acceso no autorizado a la base de datos de ciudadanos, el Ransomware en los servidores institucionales, la modificación de la información del sistema PQRS y la fuga de información ocasionada por el uso compartido de credenciales. Estos riesgos se clasificaron con un nivel alto debido a que combinan un impacto significativo sobre la operación institucional y una alta probabilidad de ocurrencia, de acuerdo con los principios de gestión del riesgo establecidos en la norma ISO 31000 (ISO, 2018).

El acceso no autorizado a la base de datos de ciudadanos representa uno de los riesgos más críticos porque compromete información personal administrada por la alcaldía. La materialización de este riesgo puede ocasionar la divulgación, modificación o eliminación de datos, afectando la confidencialidad y la integridad de la información. Además, puede generar incumplimiento de la normativa colombiana sobre protección de datos personales, sanciones administrativas y pérdida de confianza por parte de la ciudadanía.

El Ransomware en los servidores institucionales presenta otro riesgo prioritario debido a que estos equipos alojan aplicaciones y bases de datos indispensables para el funcionamiento de la administración municipal. Un ataque exitoso podría cifrar la información, interrumpir los servicios y afectar la continuidad de procesos como la atención al ciudadano, la gestión documental y la administración financiera. La existencia de servidores sin actualizar incrementa la probabilidad de explotación de vulnerabilidades, situación que coincide con las amenazas más frecuentes identificadas actualmente (ENISA, 2023). La modificación no autorizada de la información del sistema PQRS también presenta un nivel de riesgo alto porque afecta directamente la integridad de los registros institucionales. La alteración de peticiones, quejas, reclamos y solicitudes puede generar inconsistencias en la gestión administrativa, retrasos en la atención a los ciudadanos e incluso posibles responsabilidades disciplinarias o legales para la entidad.
La fuga de información por compartir credenciales o información confidencial representa igualmente un riesgo prioritario. El uso inadecuado de las credenciales dificulta la trazabilidad de las acciones realizadas en los sistemas y aumenta la posibilidad de accesos indebidos. Esta situación se ve agravada por la escasa cultura de ciberseguridad identificada durante el diagnóstico, lo que incrementa la exposición a ataques de ingeniería social y al uso incorrecto de los recursos tecnológicos.
Por su parte, el phishing dirigido a funcionarios fue valorado con un impacto medio y una probabilidad alta, debido a que el correo electrónico continúa siendo uno de los principales medios utilizados por los ciberdelincuentes para obtener credenciales de acceso. Aunque inicialmente el impacto puede ser limitado a una cuenta comprometida, sus consecuencias pueden escalar rápidamente y facilitar otros ataques contra la infraestructura tecnológica de la alcaldía (ENISA, 2023).
La caída de servicios por fallas de infraestructura fue clasificada como un riesgo de nivel medio. Aunque puede afectar temporalmente la disponibilidad de los sistemas institucionales, la implementación de medidas como copias de seguridad, sistemas de alimentación ininterrumpida (UPS), mantenimiento preventivo y planes de recuperación puede reducir significativamente sus efectos sobre la operación de la entidad.
Los resultados de la matriz permiten establecer que la prioridad de la Alcaldía Municipal Villa Nuevo Sol debe centrarse en fortalecer los controles de acceso, mejorar la protección de los servidores, implementar programas permanentes de capacitación en ciberseguridad, verificar periódicamente las copias de seguridad y establecer mecanismos de monitoreo continuo. Estas acciones contribuirán a reducir tanto la probabilidad de ocurrencia como el impacto de los riesgos identificados, fortaleciendo la seguridad de la información y garantizando la continuidad de los servicios públicos (ISO, 2022).

Políticas y controles de seguridad

Políticas propuestas

Tabla 5. Políticas de seguridad

Política	***Objetivo***	***Riesgo asociado***

Política de gestión de usuarios y contraseñas	Garantizar que los usuarios autorizados accedan a los sistemas institucionales por medio de credenciales seguras	Acceso no autorizado al sistema y la base de datos
Política de seguridad sobre el correo institucional	Establecer reglas para el uso seguro del correo y prevenir ataques de phishing	Robo de credenciales y/o phishing
Política de manejo de los datos	Estandarizar niveles de clasificación y controles para proteger la información y los datos de los ciudadanos	Divulgación o fuga de información confidencial
Política sobre las copias de seguridad	Priorizar la disponibilidad de la información por medio de respaldos periódicos y verificarlos al momento de restaurar	Pérdida de información y continuidad del servicio
Política para el uso de dispositivos institucionales transportables	Controlar el uso de memorias y dispositivos para evitar fuga de información o ingreso de malware	Malware y fuga de información
Política de continuidad y disponibilidad de los servicios	Garantizar la disponibilidad de los sistemas institucionales ante fallas técnicas, eléctricas o ataques de Ransomware	Caída de servicios por fallas de infraestructura / Ransomware

Controles propuestos

Tabla 6. Controles de seguridad

Riesgo	***Control***	***Justificación***
Acceso no autorizado a los sistemas	Verificación doble y revisión periódica de privilegios de acceso	Reduce la probabilidad de accesos indebidos por credenciales compartidas
Phishing	Filtros antispam y campañas de capacitación periódicas	Baja la probabilidad de robo de credenciales e ingeniería social
Ransomware en servidor	Actualización periódica del sistema, antivirus y copias de seguridad verificables	Reduce la explotación de vulnerabilidades y facilita la recuperación
Robo o pérdida de un equipo	Control de acceso físico, cámaras, inventario y registro de salida de equipos	Disminuye el riesgo de pérdida de equipos con información institucional
Interrupción del servicio por fallas técnicas	Instalación de UPS y planta eléctrica para servidores críticos	Mantiene la continuidad de operaciones ante fallas eléctricas
Modificación no autorizada del sistema PQRS	Registros de auditoría (logs) de cambios y restricción de permisos de edición por rol	Permite detectar y revertir modificaciones no autorizadas, reforzando la integridad de los registros

La implementación de políticas y controles de seguridad es un elemento fundamental para fortalecer la protección de la información en la Alcaldía Municipal Villa Nuevo Sol. Después de identificar los riesgos asociados con el acceso no autorizado a los sistemas, el phishing, el Ransomware, la fuga de información y las fallas de infraestructura, es necesario establecer medidas preventivas y correctivas que permitan disminuir tanto la probabilidad de ocurrencia como el impacto de estos eventos. De acuerdo con la norma **ISO/IEC 27001:2022**, las organizaciones deben implementar un Sistema de Gestión de

Seguridad de la Información (SGSI) basado en políticas, procedimientos y controles que protejan los activos de información de manera sistemática (ISO, 2022).

Uno de los mecanismos más importantes para controlar el acceso a la información institucional son las políticas de gestión de usuarios y contraseñas. Se propone que en la alcaldía cada funcionario tenga un usuario individual (no cuentas compartidas, como se identificó en el diagnóstico), con contraseñas de mínimo ocho caracteres que se cambien cada 90 días, y que las áreas de hacienda y sistemas utilicen autenticación multifactorial por manejar la información más sensible de la entidad. Con esto disminuye considerablemente el riesgo de accesos no autorizados y se puede identificar qué usuario realizó cada acción dentro de los sistemas. El correo electrónico continúa siendo uno de los principales medios utilizados por los ciberdelincuentes para obtener credenciales; por ello, se recomienda que la alcaldía active filtros antispam y programe capacitaciones semestrales para que los funcionarios identifiquen correos sospechosos y reduzcan el riesgo de ataques de phishing (ENISA, 2023).

La correcta clasificación de la información institucional ayuda a reducir el riesgo de divulgación no autorizada. En el caso de la alcaldía, se debería clasificar como información confidencial los datos de los ciudadanos almacenados en el sistema PQRS y las bases tributarias, restringiendo su acceso únicamente al personal autorizado de cada dependencia. Esto fortalece el cumplimiento de la Ley Estatutaria 1581 de 2012 sobre protección de datos personales y de las buenas prácticas establecidas para la gestión de la seguridad de la información (ISO, 2022).

Se propone que la alcaldía programe respaldos automáticos diarios para las bases de datos de recaudos e impuestos y respaldos semanales para el archivo central y el sistema PQRS, almacenando una copia en un disco externo y otra en la nube para evitar la pérdida de información en caso de una falla del servidor. Además, se sugiere realizar una prueba de restauración cada tres meses para verificar que las copias de seguridad sean funcionales y permitan recuperar la información cuando sea necesario (ISO, 2022).

También se debe controlar el uso de dispositivos como computadores portátiles y memorias USB utilizados por algunos funcionarios para trabajar fuera de la alcaldía. Se recomienda cifrar la información de los equipos portátiles que salen de las instalaciones y restringir el uso de memorias USB personales en los computadores conectados a la red institucional, ya que estos dispositivos pueden convertirse en un medio de propagación de malware o de fuga de información. Además de las políticas institucionales, se requieren controles técnicos y administrativos, como la instalación de antivirus en todos los equipos, la actualización permanente del sistema PQRS y de los servidores con los últimos parches de seguridad, y la implementación de filtros para el correo institucional.

Entre los controles administrativos se recomienda capacitar al personal en temas de ciberseguridad y definir claramente los responsables de cada sistema, ya que el error humano continúa siendo una de las principales causas de los incidentes de seguridad (ENISA, 2023). Los controles físicos también son importantes para la sala de servidores. Se recomienda instalar cámaras de vigilancia, restringir el acceso únicamente al personal autorizado, mantener un inventario actualizado de los equipos y llevar un registro de préstamo o retiro de dispositivos. Asimismo, contar con una UPS para los servidores

críticos ayudará a evitar daños en la información y en los equipos ante interrupciones del suministro eléctrico.

Las políticas y controles propuestos conforman un sistema de protección que fortalece la seguridad de la información en la Alcaldía Municipal Villa Nuevo Sol. La implementación de estas medidas permitirá reducir la probabilidad de materialización de los riesgos identificados, mejorar la capacidad de respuesta ante incidentes y garantizar la continuidad de los servicios prestados a la ciudadanía (ISO, 2022).

Gestión de incidentes y continuidad del negocio

.

Tabla 7. Incidentes potenciales

Incidente	***Descripción***	***Impacto***

Acceso no autorizado a la base de datos de ciudadanos	Un usuario sin permisos accede por medio de credenciales comprometidas	Alto
Ataque de phishing	El funcionario recibe un correo malicioso que busca obtener sus credenciales	Alto
Ransomware en servidores	Malware que cifra la información de los servidores dejando los archivos inservibles	Alto
Fuga de información	Divulgar de manera accidental o intencional los datos personales de los ciudadanos	Alto
Modificación de documentos oficiales	Alterar o modificar sin autorización los registros administrativos institucionales	Alto
Caída de servicios por fallas de infraestructura.	Interrupción del funcionamiento de los sistemas institucionales por fallas eléctricas o técnicas	Medio

Tabla 8. Plan básico de respuesta

Fase	***Acción***

Detección	Se identifica el incidente, registrar el suceso y confirmar que tanto se afectó
Contención	Separar los sistemas que están comprometidos y así evitar la propagación y conservar la evidencia.
Erradicación	Eliminar todas las posibles causas del incidente y así corregir las posibles vulnerabilidades y actualizar los sistemas afectados.
Recuperación	Restaurarla información por medio de las copias de seguridad revisadas previamente que no estén corruptas y poder restaurar el sistema.
Lecciones aprendidas	Se deben de documentar los incidentes, Identificar las oportunidades de mejora y poder actualizar las políticas con los controles de seguridad.

- La gestión de incidentes de seguridad es un proceso fundamental para proteger la información y garantizar la continuidad de las operaciones de la Alcaldía Municipal Villa Nuevo Sol. Debido a que la entidad administra datos personales de los ciudadanos y presta servicios públicos esenciales, cualquier incidente de seguridad puede afectar la disponibilidad de los sistemas, la integridad de la información y la confianza de la comunidad. Por esta razón, es indispensable establecer procedimientos que permitan detectar, contener, erradicar y recuperar oportunamente los servicios afectados, de acuerdo con las buenas prácticas de gestión de incidentes y continuidad del negocio (ISO, 2023; ISO, 2019).
- Los incidentes identificados muestran que las principales amenazas para la alcaldía están relacionadas con el acceso no autorizado a la información, los ataques de phishing, el Ransomware, la fuga de información y la modificación de documentos oficiales, especialmente en el sistema PQRS y las bases tributarias. Estos eventos fueron clasificados con un impacto alto debido a que pueden comprometer la confidencialidad, integridad y disponibilidad de los activos de información, además de afectar el cumplimiento de las funciones institucionales y las obligaciones legales. Se propone que la detección de incidentes en la alcaldía

se apoye en la revisión diaria de los registros de acceso del servidor por parte del área de sistemas y que se habilite un correo o línea directa donde los funcionarios puedan reportar cualquier actividad sospechosa detectada en sus equipos o cuentas. Cuanto más rápido se identifique un evento sospechoso, menor será la posibilidad de que el incidente genere un impacto mayor (ISO, 2023).

- Cuando se confirme un incidente, por ejemplo, un equipo infectado con Ransomware, lo primero que se debe hacer es desconectarlo de la red institucional para evitar que se propague hacia el servidor central o hacia otros computadores de la misma dependencia. Si el incidente involucra una cuenta comprometida, esta debe bloquearse de inmediato y cambiar la contraseña. Si afecta un servicio específico, como el PQRS, se debe restringir el acceso hasta confirmar que el incidente ha sido controlado. También es importante conservar evidencias, como capturas de pantalla, registros y correos electrónicos, para apoyar el análisis posterior (ISO, 2023).
- Una vez contenido el incidente, sigue la fase de erradicación, que consiste en eliminar completamente la causa del problema mediante la eliminación de archivos maliciosos, la corrección de configuraciones inadecuadas, la actualización del sistema operativo y de las aplicaciones del servidor, así como el cambio de todas las credenciales comprometidas. Solo después de estas acciones el sistema podrá volver a operar de manera segura (ISO, 2023).
- Para la recuperación, se recomienda que la alcaldía restaure la información desde las copias de seguridad previamente verificadas, comprobando que los datos recuperados sean completos y correctos antes de poner nuevamente en funcionamiento el sistema PQRS y las bases de datos institucionales. Asimismo, se debe mantener un monitoreo durante los días posteriores para confirmar que el incidente fue completamente solucionado y no vuelva a presentarse (ISO, 2019).
- Al finalizar la atención del incidente, se sugiere que el área de sistemas documente lo ocurrido, identifique las causas, registre las lecciones aprendidas y actualice las políticas y procedimientos cuando sea necesario. Además, conviene programar capacitaciones con los funcionarios de la dependencia afectada para evitar que la situación vuelva a repetirse, ya que el error humano continúa siendo una de las principales causas de los incidentes de seguridad. También se recomienda definir los servicios críticos de la alcaldía, asignar responsables para cada uno y realizar pruebas periódicas del plan de continuidad del negocio, apoyándose en sistemas de alimentación ininterrumpida (UPS) para los servidores principales (ISO, 2019).
- Mantener un monitoreo constante, realizar mantenimiento preventivo a los equipos y actualizar periódicamente los sistemas ayuda a que la alcaldía pueda anticiparse a los incidentes antes de que ocurran, en lugar de reaccionar únicamente cuando ya se han materializado. Estas acciones, junto con la capacitación continua del personal, fortalecen la seguridad institucional y reducen el riesgo asociado al factor humano (ISO, 2022).
- En conclusión, aplicar un proceso estructurado de gestión de incidentes y un plan de continuidad del negocio permitirá a la Alcaldía Municipal Villa Nuevo Sol

responder oportunamente a los eventos que comprometan la seguridad de la información, reduciendo su impacto, facilitando la recuperación de los servicios y fortaleciendo la confianza de la ciudadanía (ISO, 2023; ISO, 2019).

Tabla 9. Hallazgos organizacionales

Situación observada	***Riesgo asociado***
No existen políticas formales de seguridad sobre la información	No se aplican los controles y aumentos de incidentes de seguridad.
Funcionarios comparten credenciales de acceso a los sistemas	Acceso no autorizado
Escasa capacitación en ciberseguridad	Robo de credenciales por medio de ingeniería social
No hay un procedimiento formal para que se reporten incidentes	Demora en respuestas a mayor impacto de los incidentes.
Uso indebido de dispositivos USB	Posible infección por algún malware y una posible fuga de información.
Escasa sensibilización sobre la protección de datos personales	Incumplimiento de las leyes y que se divulgue la información que es confidencial.

Tabla 10. Recomendaciones de mejora

Hallazgo	***Recomendación***

Ausencia de políticas de seguridad.	Crear y aprobar las políticas que estén alineadas con la norma ISO 27001
Uso compartido de credenciales.	Cuentas individuales, autenticación doble y mantener una campaña de concientización sobre el uso adecuado de las contraseñas o credenciales
Falta de capacitación.	Realizar capacitación, simulaciones sobre phishing y una jornada de sensibilización para todos los implicados con la alcaldía.
Ausencia de un procedimiento para fallos.	Crear reglas para realizar reportes, registros, y atención sobre fallos que comprometan la seguridad
Uso de dispositivos USB.	Prohibir el uso de dispositivos externos e implementar configuraciones para prevenir que se divulgue información confidencial.
Una baja cultura de protección de datos personales.	Crear campañas sobre la confidencialidad y el tratamiento de los datos personales y las responsabilidades que lleva cada funcionario.

La cultura organizacional en ciberseguridad es el conjunto de valores, conocimientos, comportamientos y prácticas que orientan la forma en que los funcionarios protegen la información y utilizan los recursos tecnológicos de la organización. En la Alcaldía Municipal Villa Nuevo Sol, el análisis realizado permitió identificar diversas situaciones que aumentan la exposición a incidentes de seguridad, principalmente relacionadas con la ausencia de políticas formales, la limitada capacitación del personal y la falta de procedimientos para la gestión de incidentes. Estas condiciones muestran la necesidad de fortalecer la cultura organizacional para que la seguridad de la información sea una responsabilidad de todos los funcionarios y no solo del área de tecnología (ISO, 2022).

La inexistencia de lineamientos claros de seguridad genera que cada funcionario actúe según su propio criterio, lo que ocasiona inconsistencias en la aplicación de controles y aumenta la probabilidad de incidentes. Se propone que la alcaldía redacte y apruebe una política formal de seguridad de la información donde queden definidas las responsabilidades de cada dependencia y las normas básicas para el uso de los equipos, el correo institucional y el acceso a los sistemas como el PQRS. De esta manera, todos los funcionarios conocerán las reglas que deben cumplir para reducir los riesgos en el manejo de la información (ISO, 2022).

Otro aspecto crítico identificado es el uso compartido de credenciales, práctica detectada principalmente en áreas como Hacienda y Sistemas. Esta situación dificulta identificar quién realizó cada acción dentro de los sistemas institucionales y facilita los accesos no autorizados. Por ello, se recomienda que cada funcionario disponga de un usuario individual, que las áreas más sensibles utilicen autenticación multifactorial y que se desarrollen campañas de sensibilización sobre el uso adecuado de las credenciales.

Asimismo, la escasa capacitación en ciberseguridad incrementa la vulnerabilidad frente a amenazas como el phishing y la ingeniería social. Se propone realizar al menos dos jornadas de capacitación al año, incluyendo simulaciones de phishing dirigidas a las dependencias que administran información más sensible (ENISA, 2023).

El diagnóstico también mostró que no existe un procedimiento formal para reportar incidentes. Cuando un funcionario desconoce cómo actuar frente a una situación sospechosa, aumenta el tiempo de respuesta y el impacto del incidente. Se recomienda establecer un canal oficial de reporte, como un correo electrónico o una línea directa con el área de sistemas, además de definir un procedimiento claro que indique a quién informar y qué acciones seguir después del reporte (ISO, 2022).

El uso inadecuado de dispositivos USB y otros medios de almacenamiento externos constituye otro riesgo importante, ya que estos dispositivos pueden introducir software malicioso o facilitar la salida no autorizada de información confidencial. Se recomienda restringir el uso de dispositivos USB personales y permitir únicamente aquellos autorizados y previamente revisados por el área de sistemas.

La escasa sensibilización sobre la protección de datos personales también representa una oportunidad de mejora, dado que la alcaldía administra información de los ciudadanos y tiene responsabilidades legales sobre su tratamiento. Por ello, se recomienda incluir dentro de las capacitaciones un módulo específico sobre la Ley Estatutaria 1581 de 2012, con el fin de que los funcionarios conozcan qué información pueden compartir, con quién y en qué condiciones.

Fortalecer esta cultura organizacional también requiere el compromiso de la alta dirección. El alcalde y los secretarios deben respaldar la asignación de recursos para implementar las políticas, controles y programas de capacitación, promoviendo la participación de todos los funcionarios. El liderazgo institucional favorece la adopción de buenas prácticas y el cumplimiento de los objetivos de seguridad de la información (ISO, 2022).

Las recomendaciones propuestas contribuirán al fortalecimiento de la cultura organizacional en la Alcaldía Municipal Villa Nuevo Sol. Implementar políticas claras, desarrollar programas de capacitación, definir procedimientos para reportar incidentes, fortalecer la protección de datos personales y promover buenas prácticas permitirá reducir la probabilidad de incidentes y mejorar la capacidad de respuesta de la organización, fortaleciendo así la confianza de la ciudadanía en la administración municipal (ISO, 2022; ENISA, 2023).

Conclusiones

1. El análisis realizado permitió identificar que la Alcaldía Municipal Villa Nuevo Sol tiene debilidades importantes en la gestión de la seguridad de la información, principalmente relacionadas con la ausencia de políticas formales, el uso compartido de credenciales, la poca capacitación del personal y la falta de procedimientos estructurados para la gestión de incidentes. Estas condiciones aumentan la probabilidad de que amenaces como el acceso no autorizado, el phishing, el Ransomware y la fuga de información afecten el funcionamiento de la entidad y la prestación de los servicios a la ciudadanía.
2. La base de datos de ciudadanos, el sistema de PQRS, los servidores institucionales y la red informática resultaron ser los activos más críticos para la operación de la alcaldía, según la identificación y valoración que se hizo. Proteger estos activos debería ser una prioridad institucional, ya que cualquier afectación sobre ellos puede comprometer la continuidad de los servicios públicos, la confianza de los ciudadanos y el cumplimiento de las obligaciones legales relacionadas con la protección de la información.
3. Los riesgos con mayor prioridad, según la metodología de análisis aplicada, corresponden al acceso no autorizado a los sistemas, los ataques de Ransomware, el phishing y la fuga de información. Valorar el impacto y la probabilidad de cada uno ayudo a priorizar las acciones de tratamiento, lo que demuestra que es importante tener un enfoque preventivo para poder enfocar los recursos disponibles hacia los riesgos que representan una mayor amenaza para la organización.
4. Proponer políticas de seguridad, controles administrativos, técnicos y físicos, junto con un plan básico para la gestión de incidentes y la continuidad del negocio, es una oportunidad para fortalecer bastante la postura de ciberseguridad de la alcaldía. Poner en marcha estas medidas permitirá reducir la probabilidad de que ocurran incidentes, mejorar la capacidad de respuesta ante eventos de seguridad y garantizar una recuperación más eficiente de los servicios institucionales cuando se presenten situaciones de contingencia.
5. El diagnóstico realizado confirma que la seguridad de la información en la Alcaldía Municipal Villa Nuevo Sol depende tanto de la implementación de controles técnicos como del fortalecimiento de la cultura organizacional identificado en el análisis, incluyendo el compromiso de la alta dirección y la capacitación permanente de los funcionarios. Consolidar estas acciones permitirá avanzar hacia una gestión de la seguridad de la información orientada a la mejora continua, conforme a lo establecido en la ISO/IEC 27001:2022, favoreciendo la protección de los activos institucionales y el cumplimiento de la misión de la entidad.

Referencias

- Congreso de Colombia. (2009). *Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.*
- Congreso de Colombia. (2012). *Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.*
- European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape 2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
- International Organization for Standardization. (2018). *ISO 31000:2018 Risk management — Guidelines.*
- International Organization for Standardization. (2019). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.*
- International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*
- International Organization for Standardization. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls.*
- International Organization for Standardization. (2022). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.*
- International Organization for Standardization. (2023). *ISO/IEC 27035-1:2023 — Information technology: Information security incident management — Part 1: Principles and process*. https://www.iso.org/standard/78973.html
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). *Modelo de Seguridad y Privacidad de la Información (MSPI).* https://www.mintic.gov.co/portal/inicio/Seguridad-y-Privacidad-de-la-Informacion/
- National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2).* https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* https://doi.org/10.6028/NIST.CSWP.29