

ANÁLISIS SOBRE LAS VULNERABILIDADES EN LA INFRAESTRUCTURA DE TI  
DE LAS ENTIDADES TERRITORIALES DE SEXTA CATEGORÍA (ALCALDÍAS)  
EN TERRITORIO COLOMBIANO.

LUIS ALBERTO HOLGUIN CARVAJAL

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

2024

ANÁLISIS SOBRE LAS VULNERABILIDADES EN LA INFRAESTRUCTURA DE TI  
DE LAS ENTIDADES TERRITORIALES DE SEXTA CATEGORÍA (ALCALDÍAS)  
EN TERRITORIO COLOMBIANO.

LUIS ALBERTO HOLGUIN CARVAJAL

Proyecto de Grado – Monografía presentada para optar por el título de  
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Hernando José Peña Hidalgo

Asesor – opción de grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI  
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA  
CIP- DOSQUEBRADAS, RISARALDA

2024

## NOTA DE ACEPTACIÓN

---

---

---

---

---

---

---

---

---

Firma del Presidente de Jurado

---

Firma del Jurado

---

Firma del Jurado

Fecha: 12 de Diciembre de 2024.

## DEDICATORIA

Dedico este trabajo de grado a mis padres, hermana y esposa, que han estado presentes en cada aspecto que ha comprendido mi formación profesional, por su apoyo incondicional, que ha servido cada día como motivación para alcanzar un peldaño más, y lograr esta meta como especialista, en una ciencia que amo y respeto, como lo es la tecnología, la ciencia, el desarrollo y la seguridad digital, como una sinergia para el apoyo del crecimiento constante de la sociedad; por ello siempre estaré fortalecido y guiado por los mejores Padres; Alberto y Luz Mila; mi Hermanita Johana y; mi incondicional esposa Marcela. Para ellos siempre mis más sentidos agradecimientos.

*Por  
Luis Alberto Holguin Carvajal  
Ingeniero de Sistemas*

## CONTENIDO

|                                                   | Pág. |
|---------------------------------------------------|------|
| INTRODUCCIÓN.....                                 | 14   |
| 1. DEFINICIÓN DEL PROBLEMA .....                  | 15   |
| 1.1.ANTECEDENTES DEL PROBLEMA.....                | 15   |
| 1.2.FORMULACIÓN DEL PROBLEMA .....                | 17   |
| 2. JUSTIFICACIÓN .....                            | 18   |
| 3. OBJETIVOS .....                                | 20   |
| 3.1.OBJETIVO GENERAL.....                         | 20   |
| 3.2.OBJETIVOS ESPECÍFICOS .....                   | 20   |
| 4. MARCO REFERENCIAL .....                        | 21   |
| 4.1.MARCO TEÓRICO.....                            | 21   |
| 4.2.MARCO CONCEPTUAL.....                         | 24   |
| 4.2.1. Sistemas de información. ....              | 24   |
| 4.2.2. Infraestructura de TI. ....                | 24   |
| 4.2.3. Redes de datos. ....                       | 25   |
| 4.2.4. Seguridad digital. ....                    | 25   |
| 4.2.5. Ente territorial.....                      | 25   |
| 4.2.6. Categoría de los entes territoriales. .... | 26   |
| 4.3.MARCO HISTÓRICO .....                         | 26   |
| 4.3.1. Los primeros ciberataques. ....            | 26   |
| 4.3.2. Otros Elementos. ....                      | 27   |
| 4.3.3. Puntualización.....                        | 28   |
| 4.4.ESTADO ACTUAL .....                           | 29   |
| 4.5.MARCO TECNOLÓGICO.....                        | 30   |
| 4.5.1. Firewalls.....                             | 30   |
| 4.5.2. Seguridad del correo electrónico. ....     | 30   |
| 4.5.3. Segmentación de la red.....                | 30   |

|                                                                                                                                                                |    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 4.5.4. Control de acceso. ....                                                                                                                                 | 30 |
| 4.5.5. Seguridad inalámbrica.....                                                                                                                              | 31 |
| 4.6. MARGO LEGAL .....                                                                                                                                         | 31 |
| 5. DESARROLLO DE LOS OBJETIVOS .....                                                                                                                           | 33 |
| 5.1. BRECHAS DE SEGURIDAD DE LOS ENTES TERRITORIALES<br>ESPECÍFICAMENTE ALCALDÍAS .....                                                                        | 33 |
| 5.1.1. Brechas de seguridad .....                                                                                                                              | 33 |
| 5.1.2. Posibles eventos de vulnerabilidad. ....                                                                                                                | 35 |
| 5.1.3. Modelos análisis de riesgo. ....                                                                                                                        | 37 |
| 5.1.4. Gestión de activos de información.....                                                                                                                  | 37 |
| 5.2. ANTECEDENTES, DE EVENTOS DE VULNERABILIDADES PRESENTADOS<br>EN LAS ENTIDADES DE ORDEN TERRITORIAL DE CATEGORÍA SEXTA,<br>ESPECÍFICAMENTE ALCALDÍAS .....  | 38 |
| 5.3. MODELO DE ANÁLISIS Y GESTIÓN DEL RIESGO BASADO EN LAS<br>CARACTERÍSTICAS DE INFRAESTRUCTURA TI .....                                                      | 40 |
| 5.3.1. Objetivo.....                                                                                                                                           | 41 |
| 5.3.2. Metodología .....                                                                                                                                       | 41 |
| 5.3.3. Tipos de Activos .....                                                                                                                                  | 43 |
| 5.3.4. Amenazas .....                                                                                                                                          | 49 |
| 5.3.5. Correlación de errores y ataques metodología magerit .....                                                                                              | 68 |
| 5.4. BUENAS PRÁCTICAS QUE PERMITAN GESTIONAR EL RIESGO BASADO<br>EN ESTÁNDARES CON EL FIN GESTIONAR LA SEGURIDAD DE LA<br>INFORMACIÓN EN ESTAS ENTIDADES. .... | 71 |
| 5.4.1. Recomendaciones generales sobre activos de información: .....                                                                                           | 74 |
| 5.4.2. Fichas de control para activos esenciales .....                                                                                                         | 75 |
| 5.4.3. Descripción del mapa de riesgos.....                                                                                                                    | 76 |
| 6. CONCLUSIONES.....                                                                                                                                           | 78 |
| 7. RECOMENDACIONES .....                                                                                                                                       | 80 |
| 7.1. RECOMENDACIONES GENERALES .....                                                                                                                           | 80 |
| 7.1.1. Contar con el apoyo de la alta gerencia .....                                                                                                           | 80 |
| 7.1.2. Involucrar a todas las partes interesadas .....                                                                                                         | 80 |

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| 7.1.3. Establecer una cultura de seguridad .....                                  | 80 |
| 7.1.4. Implementar controles efectivos .....                                      | 81 |
| 7.1.5. Realizar auditorías periódicas .....                                       | 81 |
| 7.2. RECOMENDACIONES ESPECIFICAS .....                                            | 81 |
| 7.2.1. Adaptar las medidas a las características específicas de la alcaldía ..... | 81 |
| BIBLIOGRAFÍA.....                                                                 | 83 |
| 8. ANEXO.....                                                                     | 87 |

## LISTA DE TABLAS

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| Tabla 1. Amenazas .....                                                         | 49 |
| Tabla 2. Fuego .....                                                            | 49 |
| Tabla 3. Daños por agua .....                                                   | 49 |
| Tabla 4. Desastres naturales .....                                              | 50 |
| Tabla 5. Origen industrial .....                                                | 50 |
| Tabla 6. Daños por agua. ....                                                   | 50 |
| Tabla 7. Desastres naturales .....                                              | 51 |
| Tabla 8. Contaminación mecánica .....                                           | 51 |
| Tabla 9. Contaminación electromagnética .....                                   | 51 |
| Tabla 10. Avería de origen físico o lógico .....                                | 52 |
| Tabla 11. Corte del suministro eléctrico .....                                  | 52 |
| Tabla 12. Condiciones inadecuadas de temperatura .....                          | 52 |
| Tabla 13. Fallo de servicios de comunicaciones .....                            | 53 |
| Tabla 14. Interrupción de otros servicios y suministros esenciales .....        | 53 |
| Tabla 15. Degradación de los soportes de almacenamiento de la información ..... | 53 |
| Tabla 16. Emanaciones electromagnéticas .....                                   | 54 |
| Tabla 17. Errores de los usuarios .....                                         | 55 |
| Tabla 18. Errores del administrador .....                                       | 55 |
| Tabla 19. Errores del monitorización .....                                      | 55 |
| Tabla 20. Errores de configuración .....                                        | 56 |
| Tabla 21. Deficiencias en la organización .....                                 | 56 |
| Tabla 22. Difusión de software dañino .....                                     | 56 |
| Tabla 23. Errores de encaminamiento .....                                       | 57 |
| Tabla 24. Errores de secuencia .....                                            | 57 |
| Tabla 25. Escapes de información .....                                          | 57 |
| Tabla 26. Alteración accidental de la información .....                         | 58 |
| Tabla 27. Destrucción de la información .....                                   | 58 |
| Tabla 28. Fugas de información.....                                             | 58 |
| Tabla 29. Vulnerabilidades de los programas .....                               | 59 |
| Tabla 30. Errores de mantenimiento .....                                        | 59 |
| Tabla 31. Caída del sistema por agotamiento de recursos .....                   | 59 |
| Tabla 32. Robo .....                                                            | 60 |
| Tabla 33. Manipulación de los registros de actividad .....                      | 60 |
| Tabla 34. Manipulación de la configuración .....                                | 61 |
| Tabla 35. Suplantación de la identidad del usuario .....                        | 61 |
| Tabla 36. Abusos de privilegios de acceso .....                                 | 61 |

|                                                                              |    |
|------------------------------------------------------------------------------|----|
| Tabla 37. Uso no previsto .....                                              | 62 |
| Tabla 38. Difusión de software dañino .....                                  | 62 |
| Tabla 39. Re encaminamiento de mensajes .....                                | 62 |
| Tabla 40. Alteración de secuencia .....                                      | 63 |
| Tabla 41. Análisis de trafico .....                                          | 63 |
| Tabla 42. Repudio .....                                                      | 63 |
| Tabla 43. Interceptación de información .....                                | 64 |
| Tabla 44. Modificación deliberada de la información.....                     | 64 |
| Tabla 45. Destrucción de información .....                                   | 64 |
| Tabla 46. Revelación de información .....                                    | 65 |
| Tabla 47. Manipulación de programas .....                                    | 65 |
| Tabla 48. Manipulación de los equipos .....                                  | 65 |
| Tabla 49. Denegación de servicio .....                                       | 66 |
| Tabla 50. Robo .....                                                         | 66 |
| Tabla 51. Ataque destructivo .....                                           | 66 |
| Tabla 52. Indisponibilidad del personal .....                                | 67 |
| Tabla 53. Extorsión .....                                                    | 67 |
| Tabla 54. Ingeniería social.....                                             | 67 |
| Tabla 55. Correlación de errores y ataques metodología magerit .....         | 68 |
| Tabla 56. Ejemplo de identificación de activos y riesgos del mismo. ....     | 69 |
| Tabla 57. Parámetro de Integralidad, Confidencialidad y Disponibilidad. .... | 73 |
| Tabla 58. Formato para activos esenciales.....                               | 75 |
| Tabla 59. Formato de valorización .....                                      | 76 |
| Tabla 60. Formato de activos inferiores .....                                | 76 |

## LISTA DE FIGURAS

|                                         |    |
|-----------------------------------------|----|
| Figura 1. Activos esenciales .....      | 44 |
| Figura 2. Arquitectura de sistema ..... | 44 |
| Figura 3. Datos de información .....    | 44 |
| Figura 4. Claves criptográficas.....    | 45 |
| Figura 5. Servicios .....               | 45 |
| Figura 6. Software .....                | 46 |
| Figura 7. Hardware .....                | 46 |
| Figura 8. Redes de comunicación.....    | 47 |
| Figura 9. Soporte de información .....  | 47 |
| Figura 10. Equipamiento auxiliar.....   | 48 |
| Figura 11. Instalaciones.....           | 48 |
| Figura 12. Personal .....               | 48 |
| Figura 13. Informe de CCIT .....        | 71 |

## GLOSARIO

**VULNERABILIDAD:** Se trata de los factores que inciden en la identificación de los riesgos, donde el delincuente informático puede realizar intrusiones por medio de diferentes vectores de ataque.

**RIESGO DIGITAL:** Elementos débiles dentro de una estructura digital, la cual puede ser interpretada como una vulnerabilidad

**INCIDENCIA:** Es la ocurrencia de uno o varios eventos que puedan afectar la integridad, la confidencialidad y la disponibilidad de la información, como hechos que afectan las políticas de seguridad establecidas en una organización.

**VECTOR DE ATAQUE:** Hace referencia al método utilizado por un delincuente informático para ingresar a un determinado sistema de información.

**BACKUP:** Se trata de la información que puede ser respaldada, en proceso denominado copia de respaldo o copia de seguridad.

**AUTENTICACIÓN:** Proceso con el cual un usuario se identifica en un sistema de información.

**CERTIFICADO DIGITAL:** Hacer referencia a un documento informático generado por un prestador de servicios de certificación para garantizar la autenticidad del recurso digital al cual se está accediendo.

**CIBERSEGURIDAD:** Es la actividad o práctica que busca proteger, los activos de información, equipos, redes de datos y software, que se pueden representar como sistemas críticos para la operación de las actividades de las organizaciones.

**CRIPTOGRAFÍA:** Se trata de la protección de información por medio algoritmos que cuentan con diferentes estructuras de codificación para establecer procesos protección de datos, firmas digitales y demás elementos de privacidad o reserva.

**FIREWALL:** Sistema de seguridad de red que permite controlar y/o restringir el tráfico de una red, con fines de protección de información.

## RESUMEN

El presente análisis se proyectó hacia la identificación de los mecanismos necesarios para aplicar planes de gestión de tecnologías de TI, enfocados en las actividades que involucran la seguridad informática, por tanto se establecen de manera objetiva la normatividad que aplica en el direccionamiento estratégico de la administración de los sistemas de información en las entidades públicas, centrando el análisis en los entes territoriales de sexta categoría (alcaldías), ya que estas suelen contar con recursos económicos limitados, para el desarrollo de políticas, planes y demás factores de apropiación tecnológica, y más cuando se abordan temas de seguridad digital, por lo cual la alta dirección debe tomar medidas de gestión consecuentes con la capacidad instalada, y en beneficio institucional, con la finalidad de salvaguardar la información como un activo indispensable para el desarrollo organizacional, sin olvidar que existen atacantes informáticos, que pueden hacer uso de diversos canales o vectores, generando la probabilidad en la generación de escenarios de vulnerabilidad en las infraestructuras de TI, y más cuando no cuentan con recursos financieros importantes para el despliegue de robustos sistemas de protección de información, siendo relevante establecer protocolos que permitan establecer lineamientos de control de seguridad para mantener la integridad de la información institucional, por tanto, la presente revisión monográfica buscó establecer un análisis que permita reconocer una generalidad de las posibilidades de control sobre los diferentes riesgos en los cuales se puede ver expuesta una entidad pública, por lo cual se tratan temas de vulnerabilidad digital, vectores de ataque, ingeniería social y procesos de identificación de riesgos, como un espectro conjunto para mantener procesos de control eficaces para la seguridad digital de las entidades estatales, que cuenta con recursos limitados en el ejercicio de aplicación de la seguridad informática, donde se pueden identificar recomendaciones de adopción con menores costos de ejecución .

**Palabras clave:** Infraestructura de TI, normatividad, redes de datos, seguridad digital, tecnologías de la información

## ABSTRACT

The present analysis was projected towards the identification of the necessary mechanisms to apply IT technology management plans, focused on the activities that involve information security, therefore the regulations that apply in the strategic direction of the administration are objectively established. of information systems in public entities, focusing the analysis on sixth-category territorial entities (municipalities), since these usually have limited economic resources, for the development of policies, plans and other factors of technological appropriation, and more when digital security issues are addressed, for which top management must take management measures consistent with the installed capacity, and for the institutional benefit, in order to safeguard information as an essential asset for organizational development, without forgetting that there are computer attackers, who can make use of various channels or vectors, generating the probability of generating vulnerability scenarios in IT infrastructures, and more when they do not have significant financial resources for the deployment of robust information protection systems, being It is relevant to establish protocols that allow the establishment of security control guidelines to maintain the integrity of institutional information, therefore, the present monographic review sought to establish an analysis that allows recognizing a generality of the possibilities of control over the different risks in which it can be seeing a public entity exposed, for which digital vulnerability issues, attack vectors, social engineering and risk identification processes are addressed, as a joint spectrum to maintain effective control processes for the digital security of state entities, which counts with limited resources in the computer security application exercise, where adoption recommendations can be identified with lower execution costs .

**Keywords:** IT infrastructure, regulations, data networks, digital security, information technologies

## INTRODUCCIÓN

La seguridad digital hace parte fundamental de los procesos de control que se deben adoptar en las instituciones, por tanto Identificar las vulnerabilidades se convierte en una de las acciones que se deben priorizar en los entornos de protección de las infraestructuras de TI, pero en algunos casos de estos procesos de implementación tienden a ser costos, y el conocimiento aplicado desde una espectro ingenieril, representan limitaciones para el desarrollo objetivos de tan importantes procesos para el desarrollo fundamentado en la protección de las información, siendo consecuente con la necesidad de aplicar elementos de control y gestión como: almacenamiento en la nube, CRM, Firewall, sistemas robusto de protección de información, respaldos automatizados entre otros, por lo cual los procesos de detención temprana son vitales para este tipo de infraestructura, donde la capacidad financiera requiere de una mejor gestión acorde con la capacidad instalada, proporcionando así dinámicas que aporten al mejoramiento escalado de dicha capacidad, siendo importante la necesidad de reconocer e implementar elementos de gestión de riesgos, analizando brechas de seguridad de TI, con la finalidad de permitir generar recomendaciones y buenas prácticas en el sector.

Por lo anterior, es importante reconocer que la implementación de adecuadas medidas de seguridad representa una seria de desafíos que pueden representados en costos, conocimientos técnicos, así como la capacidad financiera institucional, por lo cual es importante fortalecer elementos que puedan estar acompañados de procesos de almacenamiento en la nube. Firewall, respaldos de información automatizados; así como establecimiento de políticas que permitan establecer procedimientos de detección temprana de amenazas, por lo cual se deben considerar las acciones de gestión de riesgos y las buenas prácticas que conlleva la seguridad digital.

## **1. DEFINICIÓN DEL PROBLEMA**

### **1.1. ANTECEDENTES DEL PROBLEMA**

Los procesos que involucran la seguridad informática en las entidades públicas son importantes para el desarrollo de actividades que son eficientes para la formulación y aplicación de políticas y planes alineados al propósito de garantizar los respectivos controles que son necesarios en la gestión de la seguridad y la privacidad de la información, donde es posible aplicar metodologías de seguridad, las cuales se encuentren en el proceso de identificación de vulnerabilidades, aportado de manera relevante como un referente de acción y apropiación de las tecnologías de información, para las entidades públicas de sexta categoría como las alcaldías que se encuentren en este orden en particular, debido de ciertas variables de disponibilidad de recursos financiero, que se pueden considerar como limitantes en los procesos de gestión y ejecución de metodologías alineadas con la seguridad informática, por tanto, la identificación y análisis de brechas de seguridad en la infraestructuras de TI, sirven como una sinergia en el desarrollo de procesos y procedimientos que involucren los modelos para actuar frente a el uso de los elementos de gestión institucional, con la finalidad de salvaguardar la información, adoptados desde la visión holística de la buenas prácticas de la gestión del riesgo.

Por lo anterior, es importante que la normatividad actual, permita establecer instrumentos que buscan incorporar herramientas que sirvan para establecer controles en las entidades públicas, por ello se reconoce el decreto 1078 de 2015 de Función Pública <sup>1</sup> en su artículo 2.2.9.1.2.2 donde se establecen instrumentos para implementar una estrategia de gobierno digital donde cada entidad pueda formular e implementar un plan estratégico de tecnologías de la información y las comunicaciones PETI <sup>2</sup>, este proceso agrupa también componentes que abordan la gestión de la infraestructura física y sus respectivos activos, seguridad en redes de datos, protocolos de contraseñas seguras aplicación de la normatividad

---

<sup>1</sup> FUNCIÓN PÚBLICA. Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones—Gestor Normativo—Función Pública [página web]. (2015). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888>

<sup>2</sup> MINTIC. [página web]. (2020). [Consultado el 30, marzo, 2023]. PETI - Arquitectura TI. <https://www.mintic.gov.co/arquitecturati/630/w3-article-9148.html>

correspondiente a la familia ISO 27000, y sus respectivas series como la ISO/ IEC 27001 y e ISO/IEC 270002, donde también confluyen los planes de seguridad y privacidad de la información así como el plan de tratamiento de riesgos de seguridad y privacidad de la información, todo esto fundamentado en el documento CONPES 3650 del 15 de marzo 2010 y CONPES 3785 de 9 de diciembre de 2013<sup>3</sup>, el cual establece la importancia de la implementación estratégica, actualmente llamada gobierno digital. En Colombia se insta al ministerio de Tecnologías de la Información y las Comunicaciones a formular las diferentes políticas que permitan un ejercicio de sostenibilidad y direccionamiento estratégico, aplicado a las diferentes instituciones públicas <sup>4</sup>.

Asimismo, las anteriores políticas se pueden articular con los procesos de gestión e identificación de vulnerabilidades; los cuales, intervienen en la medida que es necesario reconocer posibles brechas en una infraestructura tecnológica, dentro de los cuales se pueden reconocer, métodos de intrusión como: phishing, el vishing y el smishing, los cuales generan escenarios de vulnerabilidad que deben ser analizados desde la perspectiva de prevención, reconociendo la capacidad instalada de los mismas instituciones, ya que las entidades territoriales, de sexta categoría; haciendo referencia a esta clasificación debido a la asignación de recursos los cuales tienden a ser limitados, y sin notarse grandes inversiones en los aspectos de desarrollo tecnológico, lo cual conlleva a un importante ejercicio de gestión que debe ser abordado desde la alta gerencia para la adopción de políticas de TI, respaldos de información, autenticación de usuarios, gestión de activos de información, aspectos de ingeniería social, y demás que confluyan en el propósito transversal de la seguridad informática, aduciendo a metodologías ágiles, que sean objetivamente utilizadas desde la necesidad y capacidad de los entes territoriales, para minimizar el riesgo de materialización de incidentes de ciberseguridad <sup>5</sup>.

---

<sup>3</sup> MINTIC. [página web]. (2016). [Consultado el 30, marzo, 2023]. Conpes | MINCIT - Ministerio de Comercio, Industria y Turismo. Disponible en Internet: <https://www.mincit.gov.co/ministerio/normograma-sig/procesos-estrategicos/gestion-de-informacion-y-comunicacion/conpes>

<sup>4</sup> NACIONAL, Á. DE N. Y S. DE C. DEL C. C. [página web]. (2020). [Consultado el 30, marzo, 2023]. La ciberseguridad y su relevancia en el Sector Público: El papel del Centro Criptológico Nacional. Revista española de control externo.

<sup>5</sup> HOLM [página web]. (2020). [Consultado el 30, marzo, 2023]. Transformación digital en el sector público de Estonia.

## **1.2. FORMULACIÓN DEL PROBLEMA**

¿Cuáles son las brechas de seguridad más recurrentes en la infraestructura de TI en las entidades territoriales de sexta categoría (Alcaldías) en el territorio colombiano, que afectan la integridad, confidencialidad y disponibilidad en los activos de información?

## 2. JUSTIFICACIÓN

Las políticas de seguridad informática, y protección de la información , deben ser aplicables de manera transversal para direccionar a las entidades públicas de sexta categoría, en la orientación y dinamización de los diferentes procesos que soportan los planes de TI, los cuales permiten el reconocimiento y gestión de los riesgos, y por consiguiente genera la posibilidad de gestionar los recursos que se encuentren en disposición para el desarrollo de las estrategias que convergen en el beneficio de la protección de los sistemas de información, esto con la finalidad de establecer y mantener sistemas seguros, en los cuales este activo denominado información pueda mantenerse y salvaguardarse de maneja objetiva, con el cumplimiento de la normatividad y buenas prácticas existentes para tales fines <sup>6</sup>

En el presente análisis se busca la identificación de mecanismos que aporten de manera significativa a minimizar riesgos, ya que si no se logra establecer estos procesos la infraestructura de información, generará vulnerabilidades que pueden afectar la misionalidad de la institución, por lo cual, estos riesgos deben abordarse desde las condiciones técnicas de infraestructura de TI, como de una manera transversal donde se tenga presente los aspectos sociales y de comportamiento, donde se relaciona al ser humano dentro del factor de vulnerabilidad, siendo una de las falencias visibles al momento de un atacante utilizar vectores como correos electrónicos como medio de infiltración.

Por lo anterior adoptar una metodología de tipo descriptiva, permitirá reconocer estos elementos vulnerabilidad, y bajo la mirada holística de la identificación de riesgos se establecerán los mecanismos necesarios para minimizar la materialización de estas debilidades en la infraestructura de TI. Asimismo es importante abordar los temas de seguridad digital como una constante en un mundo de crecimiento tecnológico, donde las instituciones de orden público en especial los entes territoriales, debido a las limitaciones presupuestales, pueden generar escenarios donde la acción efectiva de los controles de seguridad no sean suficientes para garantizar un ejercicio sistemático de control, siendo relevante

---

<sup>6</sup> LOZANO, J. L. W.-B., & DAZA, E. F. [página web]. (2020). [Consultado el 30, marzo, 2023]. Blockchain. Disponible en: Instrumento de transparencia y control del sector público.

aportan al análisis de propuestas que contribuyan siendo el análisis monográfico un coadyuvante en el modelo de apoyo documental para comprender una realidad nacional, que puede ser visibilizada, comprendida y justificada para encontrar métodos y protocolos que sean de aporte significativo para la identificación de riesgos y por consiguiente un canal para reconocer los mismos y generar estrategias que permitan de manera objetiva al control de los riesgos, o en el mejor de los casos evitando la materialización de los mismos .

### **3. OBJETIVOS**

#### **3.1. OBJETIVO GENERAL**

Analizar las brechas de seguridad en infraestructura de TI en las entidades territoriales de sexta categoría (Alcaldía) en el territorio colombiano mediante consulta de fuentes especializadas con el fin de proponer recomendaciones y buenas prácticas que permitan gestionar el riesgo.

#### **3.2. OBJETIVOS ESPECÍFICOS**

- Inspeccionar las brechas de seguridad de los entes territoriales específicamente alcaldías, a través de informes de CSIRT Colombia, MINTIC y fuentes secundarias que permitan identificar las amenazas asociadas a las vulnerabilidades detectadas.
- Examinar antecedentes, de eventos de vulnerabilidades presentados en las entidades de orden territorial de categoría sexta, específicamente alcaldías con el fin de reconocer el impacto generado por los incidentes de seguridad identificados.
- Establecer un modelo de análisis y gestión del riesgo basado en las características de infraestructura TI de una entidad de sexta categoría, específicamente alcaldías, con el fin de identificar los activos de información críticos que se afectan la continuidad.
- Proponer recomendaciones y buenas prácticas que permitan gestionar el riesgo basado en estándares con el fin de gestionar la seguridad de la información en estas entidades.

## 4. MARCO REFERENCIAL

A continuación, se desarrollan, los elementos documentales donde se integra el contexto de la literatura que conforma el argumento del estudio, tomando como base los referentes teóricos, conceptuales, históricos, tecnológicos y legales para el desarrollo objetivo del proceso estudio que busca Analizar las brechas de seguridad en infraestructura de TI en las entidades territoriales de sexta categoría (Alcaldía) en el territorio colombiano mediante consulta de fuentes especializadas con el fin de proponer recomendaciones y buenas prácticas que permitan gestionar el riesgo .

### 4.1. MARCO TEÓRICO

La seguridad informática, es parte esencial en la protección de la información, por tanto, se abordan los sistemas de entorno seguro SSL, y TLS, con el propósito de generar mejores entornos de acuerdo con los algoritmos criptográficos<sup>7</sup>. Es de esta manera que se logran establecer los procesos que involucran la ciberseguridad adoptando medidas que sirven como complemento a los entornos seguros<sup>8</sup>. Estos elementos aportan a los sistemas de seguridad y generar controles en lo relacionado con el cibercrimen, donde los delitos informáticos, hacen parte de la correlación de acción de gestión de la seguridad informática<sup>9</sup>.

#### **Dinámica de la transformación digital entorno a la seguridad informática.**

Lo anterior permite involucrar la normatividad en el desarrollo de los modelos de seguridad, aplicando la norma ISO 27001:2013, lo cual hace referencia a la adopción de buenas prácticas en el uso de las tecnologías de la información y las comunicaciones<sup>10</sup>.

---

<sup>7</sup> CHOQUE. Análisis Comparativo De Los Algoritmos Criptográficos Utilizados En Seguridad Informática [página web]. (2022). [Consultado el 30, marzo, 2023]. Disponible en Internet: <http://ddigital.umss.edu.bo:8080/jspui/handle/123456789/29475>

<sup>8</sup> CAMILA, TRUJILLO. Casos de estudio de cibercrimen para el mejoramiento de la seguridad informática en pymes y medianas empresas - 10596/30220. Universidad Nacional Abierta y a Distancia UNAD - [página web]. (13, noviembre, 2019). [Consultado el 30, marzo, 2023]. Disponible en Internet: <http://repository.unad.edu.co/handle/10596/30220>

<sup>9</sup> PARRA CALDERÓN, J. A. [página web]. (2019). [Consultado el 30, marzo, 2023]. Delitos informáticos y marco normativo en Colombia. <http://repository.unad.edu.co/handle/10596/28115>

<sup>10</sup> RODRÍGUEZ [página web]. (2021). [Consultado el 30, marzo, 2023]. Buenas prácticas de seguridad informática aplicado al comercio electrónico para las Pymes colombianas asociada a la norma ISO 27001:2013 Anexo A. <http://repository.unad.edu.co/handle/10596/42688>

De acuerdo con Cano <sup>11</sup>, las dinámicas de las vulnerabilidades se encuentran de los vacíos de estructurales por tanto se tiene como objetivo la identificación de estas falencias en los procesos, así mismo se realizan estudios que involucren entornos de desarrollo en aplicaciones web empresariales para brindar mejores procesos de auditoría. El aumento de ataques a la seguridad informática exige en las instituciones públicas el diseño de soluciones para mejorar la seguridad tecnológica, con el fin de prevenir pérdidas de los recursos del estado, así como la información privada y sensible <sup>12</sup>.

“La Transformación Digital del Estado es una oportunidad de mejorar la productividad y el bienestar, dando a la sociedad una mayor inclusión, acceso, transparencia, calidad y cobertura de los servicios públicos. La Transformación Digital abre las puertas en la colaboración y creación de contenido, economía y negocios, tanto a nivel nacional como internacional. Este documento busca determinar las brechas entre los objetivos de Gobierno Digital”<sup>13</sup>.

Las nuevas tecnologías y el avance de estas con nuevos procesadores y la velocidad de lo que se procesa, hace que se creen nuevos programas para realizar ataques cibernéticos logrando acceder fácilmente a los datos de los usuarios aun este darse cuenta<sup>14</sup>.

Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia .

---

<sup>11</sup> CANO . La seguridad de la información en la gestión de proyectos de TI: ¿Un análisis de vulnerabilidades es suficiente? ElNotariado.com [página web]. (2016) [Consultado el 30, marzo, 2023]. Disponible en: <http://www.elnotariado.com/la-seguridad-informacion-gestion-proyectos-ti-un-analisis-vulnerabilidades-suficiente-5963.html>

<sup>12</sup> MORÁN MALDONADO, N. M. [página web]. (2021). [Consultado el 30, marzo, 2023]. Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática [BachelorThesis]. <http://dspace.ups.edu.ec/handle/123456789/20243>

<sup>13</sup> HOLM [página web]. (2020). [Consultado el 30, marzo, 2023]. Transformación digital en el sector público de Estonia: Beneficios y desafíos para la Oficina Nacional de Auditoría. Revista española de control externo, 22(64), 22-47

<sup>14</sup> FERNÁNDEZ. Reveladas siete nuevas variantes de los ataques Meltdown y Spectre [página web]. (2018). [Consultado el 30, marzo, 2023.] Disponible en: <https://instituciones.sld.cu/dnspminsap/2018/11/16/reveladas-siete-nuevas-variantes-de-los-ataques-meltdown-y-spectre/>

Los sistemas contables de las empresas son cada vez más vulnerados y estas situaciones de riesgo ponen en riesgo la información conllevando así a contrarrestar<sup>15</sup>, disminuir y controlar estos tipos de situaciones tomando como base las buenas prácticas en la aplicación de la seguridad informática en los sistemas contables<sup>16</sup>.

### **Importancia del análisis de riesgos y vulnerabilidades.**

La gestión formativa a partir de la competitividad digital genera una aplicabilidad de la seguridad informática por el uso de las tecnologías<sup>17</sup>, por tal motivo tienen un bajo conocimiento en el manejo de estas y sobre los riesgos de los ataques cibernéticos sin saber actuar ante estas situaciones dejando vulnerables los datos<sup>18</sup>.

El análisis de riesgos, así como las amenazas y vulnerabilidades propenden un establecimiento de políticas las cuales hacen referencia en los procesos que zona aplicados en el desarrollo de la normatividad ISO 27001:2013<sup>19</sup>, por tanto se la identificación de las vulnerabilidades se conjugan con las potenciales falencias de las empresa, siendo un riesgo importante de acuerdo con la seguridad de la

---

<sup>15</sup> HUAMANTINGO NAVARRO. Modelo para el análisis de vulnerabilidades digitales en una entidad pública de Lima, 2021. Repositorio Institucional - UCV. [página web]. (2022). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://repositorio.ucv.edu.pe/handle/20.500.12692/85150>

<sup>16</sup> MUÑOZ, ZAPATA, REQUENA, & RICARDO. [página web]. (2019). [Consultado el 30, marzo, 2023]. Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia. Revista Venezolana de Gerencia. <https://doi.org/10.37960/revista.v24i2.31508>

<sup>17</sup> ZAMBRANO LOOR. [página web]. (2021). [Consultado el 30, marzo, 2023]. Diseño de modelo de seguridad y plan de mejoras para la seguridad de la red, en función de las vulnerabilidades y amenazas detectadas en la empresa CENFORSP. CIA LTDA. Disponible: <https://repositorio.ecotec.edu.ec/handle/123456789/273>

<sup>18</sup> DELGADO SANTANA. Seguridad informática: Competencia digital docente en la gestión pedagógica de aula [página web]. (2022). [Consultado el 30, marzo, 2023]. Disponible en : . <http://repositorio.sangregorio.edu.ec:8080/handle/123456789/2738>

<sup>19</sup> JIMÉNEZ GARCÍA, SALAZAR BARRERA. Análisis de riesgos, amenazas y vulnerabilidades de la compañía Pinzon Pinzón & Asociados en su área de TI y planteamiento de los controles a aplicar basados en la norma ISO 27001: 2013. instname:Universidad Piloto de Colombia. [página web]. (2016). [Consultado el 30, marzo, 2023]. Disponible en Internet: <http://repository.unipiloto.edu.co/handle/20.500.12277/2727>

empresas<sup>20</sup>, algunos factores son relacionados con malware como Ransomware<sup>21</sup>, como se indica en la investigación este medio en los sistemas informáticos, lo cual obliga a la planeación y ejecución de políticas y controles de gestión que estén direccionados a la protección digital <sup>22</sup>.

La integración de las herramientas de software sirve como un modelo de acción que debe ser aplicado dentro de los procesos de fundamentación sistemática en la protección de la información<sup>23</sup>, en la medida que pueden generar la adopción de modelos como NIST para la gestión de estos protocolos<sup>24</sup>.

## **4.2. MARCO CONCEPTUAL**

**4.2.1. Sistemas de información.** Un sistema de información hace parte de una relación funcional entre tres actores importantes, los cuales se definen como recurso humano, procesos organizacionales y uso de las tecnologías de la información. Estos elementos en conjunto se denominan sistemas de información, por la acción inherente de cada uno de los actores en el proceso de gestión y administración de los activos de información .<sup>25</sup>

**4.2.2. Infraestructura de TI.** Se fundamenta en los aspectos organizacionales donde las empresas, debe desarrollar procesos operacionales y de servicios que son estructurados por medio de la acción de las tecnológica con el propósito de

---

<sup>20</sup> ODAR GUERRERO, A. Y. S. [página web]. (2018). [Consultado el 30, marzo, 2023]. Propuesta de una auditoria de seguridad para el manejo de vulnerabilidades de la red informática de la Universidad Señor de Sipan. Universidad de Lambayeque. <https://repositorio.udl.edu.pe/jspui/handle/UDL/194>

<sup>21</sup> MUÑOZ, P., & CAMILO, C. [página web]. (2019). [Consultado el 30, marzo, 2023]. Análisis de metodologías de Ethical hacking para la detección de vulnerabilidades en las Pymes. <http://repository.unad.edu.co/handle/10596/30302>

<sup>22</sup> ESCOBAR BETANCUR. Análisis de vulnerabilidades y potenciales falencias de la empresa Servicios TI frente al Ransomwar [página web]. (2019). [Consultado el 30, marzo, 2023]. Disponible en: <https://repository.uniminuto.edu/handle/10656/11150>

<sup>23</sup> SÁNCHEZ GAMBOA. Luis, [página web]. (2019). [Consultado el 30, marzo, 2023]. Identificación de vulnerabilidades y riesgos en los activos de ti de energitel. <http://repository.unad.edu.co/handle/10596/28221>

<sup>24</sup> RÍO FERNÁNDEZ. Gabriel, [página web]. (2022). [Consultado el 30, marzo, 2023]. Integración de una solución software ITSM con bases de datos de vulnerabilidades para la mejora de la ciberseguridad de las infraestructuras y sistemas TI. <https://digibuo.uniovi.es/dspace/handle/10651/64444>

<sup>25</sup> TECNOLOGÍA INFORMÁTICA. Sistema de Información. tecnología informática [página web]. (30, mayo, 2019). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://www.tecnologia-informatica.com/que-es-sistema-informacion/>>.

generar valor en los procesos desarrollados organizacionalmente, lo cual permiten la optimización y mejora continua en las actividades realizadas .<sup>26</sup>

**4.2.3. Redes de datos.** Se conoce como red de datos a la infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos. Cada una de estas redes ha sido diseñada específicamente para satisfacer sus objetivos, con una arquitectura determinada para facilitar el intercambio de los contenidos .<sup>27</sup>

**4.2.4. Seguridad digital.** “La seguridad digital es el área o disciplina encargada de proteger la infraestructura informática de una organización, así como la información que contiene, frente a posibles ataques maliciosos u otro tipo de riesgos similares.

Por tanto, la ciberseguridad o seguridad digital se encarga de proteger elementos tales como computadores, servidores, teléfonos móviles, infraestructuras de red y cualquier otro sistema informático conectado, por el que circule o en el que se almacene información valiosa para la empresa o usuario”.<sup>28</sup>

#### **4.2.5. Ente territorial**

Son entidades territoriales los departamentos, los distritos, los municipios y los territorios indígenas. La ley podrá darles el carácter de entidades territoriales a las regiones y provincias que se constituyan, en los términos de la Constitución y la ley.<sup>29</sup>

---

<sup>26</sup> IMB. ¿Qué es infraestructura de TI? IBM - Deutschland | IBM [página web]. (20, abril, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://www.ibm.com/co-es/topics/infrastructure>>.

<sup>27</sup> DEFINICIÓN. Definición de red de datos - Definicion.de. Definición.de [página web]. (13, febrero, 2019). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://definicion.de/red-de-datos/>>.

<sup>28</sup> SOTO, Leyre. ¿Qué es la seguridad digital? Welcome to the Signaturit blog [página web]. (15, abril, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://blog.signaturit.com/es/que-es-seguridad-digital>>.

<sup>29</sup> MEN. ENTIDAD TERRITORIAL: - ...:Ministerio de Educación Nacional de Colombia:... MEN - Inicio [página web]. (10, mayo, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://www.mineducacion.gov.co/1621/article-82749.html#:~:text=Z-,ENTIDAD%20TERRITORIAL%20la%20Constitución%20y%20la%20ley.>>.

**4.2.6. Categoría de los entes territoriales.** “En Colombia los distritos y municipios se clasificarán en tres grupos: grandes municipios, municipios intermedios y municipios básicos atendiendo su población, ingresos corrientes de libre destinación y situación geográfica. Los grandes municipios incluyen la categoría especial y los municipios de primera categoría. Los municipios intermedios incluyen la segunda, tercera y cuarta categoría. Los municipios básicos incluyen los de quinta y sexta categoría. Cuando los municipios deban clasificarse en una determinada categoría de acuerdo con su población, pero superan el monto de ingresos anuales señalados para esa categoría, se clasificarán en la categoría inmediatamente superior. Los municipios cuya población corresponda a una categoría determinada, pero cuyos ingresos anuales no alcancen el monto señalado para esa categoría, se clasificarán en la categoría correspondiente a sus ingresos corrientes de libre destinación anuales. Ningún municipio podrá aumentar o descender más de dos categorías entre un año y el siguiente. Los alcaldes determinarán anualmente, mediante un decreto expedido antes del 31 de octubre, la categoría en la que se encuentra clasificado para el año siguiente el respectivo distrito o municipio. La expedición de estos decretos se basará en certificaciones del Contralor General de la República sobre ingresos corrientes y del Departamento Administrativo Nacional de Estadística, Dane, sobre la población.”

En el caso de que un alcalde no expida el decreto de categorización dentro de las fechas estipuladas, esta será fijada por el Contador General de la Nación. Los municipios de frontera con población superior a 70.000 habitantes se clasificarán, como mínimo, en la cuarta categoría.<sup>30</sup>

### **4.3. MARCO HISTÓRICO**

**4.3.1. Los primeros ciberataques.** “La palabra «hacker» es anterior a los ordenadores. Antes significaba alguien incompetente en el trabajo. Entre las Líneas En la actualidad, la palabra se ha fijado en el lenguaje informático para describir a alguien que irrumpe en un sistema de forma ilegal.”<sup>31</sup> “Es su contexto histórico se le

---

<sup>30</sup> COLOMBIA ÁGIL. categoría de los entes territoriales. Colombia Agil [página web]. (21, julio, 2020). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://www.colombiaagil.gov.co/tramites/intervenciones/categorizacion-municipios>>.

<sup>31</sup> INTERNATIONAL. Historia de la Ciberseguridad. Plataforma Digital de Economía, Derecho y otras Ciencias Sociales y Humanas [página web]. (5, agosto, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://leyderecho.org/historia-de-la-ciberseguridad/>>.

atribuye el termino Hackers at play, como una termino de cuidado, por lo cual en la apoca de los 60 el FBI, se tenía asociado a situaciones delictivas, por hecho como los ocurridos en “Milwaukee 414, un grupo de jóvenes hackers acusados de entrar en más de 60 ordenadores”, donde se evidencio el acceso a los recurso informáticos del laboratorio Nacional de los Alamos, entre otros centros de investigación en salud. Estas personas fueron liberadas, ya no se contaba con una normatividad específica para el manejo de estas situaciones puntuales, por lo cual se genera una alarma frente al tema”.

**4.3.2. Otros Elementos.** “La ley se utilizó en 1988 para procesar a Robert Morris Jr., un estudiante de informática de la Universidad de Cornell que creó el «gusano» Morris, uno de los primeros programas maliciosos que infectó más de 600.000 ordenadores en instalaciones militares, académicas y de investigación médica de todo el país. Morris fue declarado culpable y condenado a tres años de libertad condicional y 400 horas de servicio comunitario y a una multa de 10.000 dólares más el coste de su supervisión.”

En 1987, el presidente Ronald Reagan firmó la Ley de Seguridad Informática, una ley más estricta que exigía directrices de seguridad para los sistemas informáticos federales, pero que limitaba el papel del Pentágono en la ciberseguridad a cuestiones de defensa nacional.

Sin embargo, al aprobar la Ley de Seguridad Informática, el Congreso rechazó la visión de la administración Reagan sobre la ley, que consistía en poner al Pentágono a cargo de la ciberseguridad tanto en el sector público como en el privado. Esto dejó a la CFAA como el modelo para la mayoría de la futura legislación sobre cibercrimen durante las siguientes tres décadas.

En 1994, por ejemplo, se modificó la CFAA para endurecer las penas de quienes transmitieran código malicioso, o malcode, como virus o gusanos informáticos. Dos años más tarde, la Ley de Protección de la Infraestructura Nacional de la Información amplió la CFAA, permitiendo el enjuiciamiento de cualquier persona que viera información informática sin autorización, independientemente de que lo hiciera con fines económicos. También en 1994, la Ley de Asistencia a las Comunicaciones para el Cumplimiento de la Ley exigía a los proveedores de

servicios de Internet que permitieran a los agentes de la ley mantener a las personas bajo vigilancia electrónica.

La Ley de Mejora de la Ciberseguridad de 2002, aprobada poco después de los atentados terroristas del 11 de septiembre, dio a los funcionarios encargados de hacer cumplir la ley un mayor acceso -sin orden judicial- a los datos personales almacenados por los proveedores de servicios de Internet. La Ley Federal de Gestión de la Seguridad de la Información, también aprobada en 2002, estableció requisitos para la protección de los sistemas y datos informáticos del gobierno.

Esas fueron las últimas medidas importantes de ciberseguridad promulgadas por el Congreso, a pesar de la presentación de numerosas propuestas durante la última década, incluidas más de 40 medidas sólo en el último Congreso. Entre las Líneas En mayo de 2011, la administración Obama envió un paquete de propuestas legislativas al Congreso. Ese paquete otorgaba al gobierno federal una nueva autoridad para garantizar que las corporaciones que poseen los activos más críticos para la seguridad y la prosperidad económica de la nación estén abordando adecuadamente los riesgos que plantean las amenazas a la ciberseguridad .

Obama y los miembros de su administración ejercieron una fuerte presión a favor del proyecto de ley. Entre las Líneas En su artículo de opinión en el Wall Street Journal, en el que instaba al Senado a aprobarlo, Obama escribió: «Gobiernos extranjeros, sindicatos criminales e individuos solitarios están sondeando nuestros sistemas financieros, energéticos y de seguridad pública todos los días».

**4.3.3. Puntualización.** Sin embargo, las diferentes opiniones sobre el papel del gobierno llevaron a la derrota de la medida. Por ello, el presidente emitió su orden ejecutiva pidiendo a las empresas de infraestructuras que adoptaran voluntariamente un conjunto mínimo de normas de seguridad creadas por el gobierno. En 1998, las autoridades descubrieron que durante un periodo de tres años se habían robado datos de los ordenadores de la NASA, los departamentos de Defensa y Energía y varios laboratorios de armamento. Nunca se demostró el origen de los ataques, apodados el «Laberinto de la Luz de la Luna», pero se sospechó del gobierno ruso, lo que convirtió el ataque en el primer caso probable

de piratería informática patrocinada por el Estado -espionaje cibernético- contra otro país.

En enero de 2000, la administración Clinton hizo pública su estrategia de ciberseguridad, que adoptaba una postura firme en cuanto a la investigación y respuesta a los ciberataques extranjeros (referido a las personas, los migrantes, personas que se desplazan fuera de su lugar de residencia habitual, ya sea dentro de un país o a través de una frontera internacional, de forma temporal o permanente, y por diversas razones) y nacionales.<sup>32</sup>

#### **4.4. ESTADO ACTUAL**

El componente que estructura la seguridad y la privacidad de la información hace parte de un modelo, el cual se comporta de manera transversal en la medida que permite conjugar elementos de gestión y administración de recursos de tecnologías de la información y las comunicaciones, esto como un enfoque que sirve como coadyuvante en el proceso que constituye tanto la formulación como la aplicación de modelos de seguridad, los cuales tengan como referente mantener la confidencialidad, así como la integralidad y la disponibilidad de la información, ya que estas condiciones permiten mantener los objetivos de misionalidad que constituyen el dinamismo estratégico dentro de una organización. Es por ello por lo que el contexto normativo, así como las herramientas que puedan servir como guías oportunas para enfocar un direccionamiento que fundamente un ejercicio pertinente en cuanto a la protección de la información, así como al mantener una correcta infraestructura tecnológica, hacen parte de los componentes que se pueden hallar dentro de los aspectos normativos que contempla en cuanto a la seguridad digital el ministerio de tecnologías de la información y las comunicaciones MINTIC.

Lo anteriormente mencionado hace parte de una conceptualización general diagnóstica, la cual sirve como antecedente en el argumento de incorporar estrategias de ciberseguridad en los entes territoriales en la medida que este dentro de los respectivos planes de mejora continua y de esta forma se pueda adoptar de manera objetiva un plan estratégico de tecnologías de la información (PETI) el cual

---

<sup>32</sup> INTERNATIONAL. Historia de la Ciberseguridad. Plataforma Digital de Economía, Derecho y otras Ciencias Sociales y Humanas [página web]. (5, agosto, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://leyderecho.org/historia-de-la-ciberseguridad/>>.

le permita generar un proceso de administración y control de los recursos digitales dispuestos por la institución partiendo de la capacidad instalada de la misma y fortaleciendo e implementando nuevas herramientas que sirvan como modelo de aplicabilidad y objetividad en el desarrollo, aportando en la protección de la información la disposición de la misma, propendiendo siempre por desarrollar procesos de transparencia salvaguardando así un ejercicio de gran importancia para las instituciones como lo es el activo de la información .

EL PETI, hace parte de un ejercicio global el cual involucra un análisis pertinente y aplicable a las diferentes infraestructuras tecnológicas de tal manera que permita determinar e incorporar nuevas tecnologías así como fortalecer las ya existentes, aportando de manera sistemática a la construcción de un camino enfocado a la modernización por medio de la gestión gerencial direccionando la misionalidad de la organización hacia una estructura convergente y propositiva que enmarca el conjunto de procesos que intervienen en la seguridad informática .

#### **4.5. MARCO TECNOLÓGICO**

**4.5.1. Firewalls.** “Sirven como barrera entre las redes de trabajo, con las redes que interactúan de manera externa”.

**4.5.2. Seguridad del correo electrónico.** “La seguridad del correo electrónico hace parte fundamental de los procesos que conforman los elementos de protección en la seguridad digital, por tanto, se deben identificar los parámetros de reducción de vulnerabilidades a los cuales se pueden estar expuesto”.

**4.5.3. Segmentación de la red.** Permita la categorización de los protocolos de acceso a la red de trabajo, permitiendo el reconocimiento de los dispositivos, generando de esta forma elementos de control y gestión.

**4.5.4. Control de acceso.** Los controles de acceso permiten establecer dinámicas de protección de las redes internas, mejorando las condiciones de seguridad institucional.

**4.5.5. Seguridad inalámbrica.** “Las redes inalámbricas no son tan seguras como las redes cableadas. Sin medidas de seguridad estrictas, instalar una LAN inalámbrica es como poner puertos Ethernet por doquier, incluso en el estacionamiento. Para evitar un ataque, necesita productos específicamente diseñados para proteger la red inalámbrica”.<sup>33</sup>

#### **4.6. MARGO LEGAL**

Es importante reconocer como los aspectos de seguridad informática se encuentran alineados dentro de un proceso que fundamenta el concepto de gobierno digital y permite adoptar una serie de normativas que son importantes para el desarrollo de procesos eficientes en el Uso de políticas, planes y estrategias alineadas al propósito de garantizar los respectivos controles que son necesarios en la gestión y administración de la seguridad y la privacidad de la información. Por ende, se reconoce el decreto 1078 de 2015<sup>34</sup> donde en su artículo 2.2.9.1.2.2 Se establecen los diferentes instrumentos para implementar una estrategia de gobierno digital donde cada entidad se pueda formular e implementar un plan estratégico de tecnologías de la información y las comunicaciones PETI, este proceso agrupa también componentes que abordan la gestión de la infraestructura física y sus respectivos activos, seguridad en redes de datos, protocolos de contraseñas seguras aplicación de la normatividad correspondiente a la familia ISO 27000, y sus respectivas series como la ISO/ IEC 27001 y e ISO/IEC 27002, donde también confluyen los planes de seguridad y privacidad de la información así como el plan de tratamiento de riesgos de seguridad y privacidad de la información, todo esto fundamentado en el documento CONPES 3650 del 15 de marzo 2010<sup>35</sup>, el cual establece la importancia de la implementación estratégica de un modelo de gobierno en línea, en Colombia se insta al ministerio de Tecnologías de la Información y las Comunicaciones a formular las diferentes políticas que permitan un ejercicio de

---

<sup>33</sup> CISCO. ¿Qué es la seguridad de red? Cisco [página web]. (15, febrero, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <[https://www.cisco.com/c/es\\_mx/products/security/what-is-network-security.html#~tipos](https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html#~tipos)>.

<sup>34</sup> DECRETO 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (2, enero, 2015). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888>>.

<sup>35</sup> CONPES | MINCIT - Ministerio de Comercio, Industria y Turismo [Anónimo]. MINCIT - Ministerio de Comercio, Industria y Turismo [página web]. (5, enero, 2010). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://www.mincit.gov.co/ministerio/normograma-sig/procesos-estrategicos/gestion-de-informacion-y-comunicacion/conpes>>.

sostenibilidad y direccionamiento estratégico desde las organizaciones e instituciones .

Asimismo, el documento CONPES 3785 de 9 de diciembre de 2013<sup>36</sup>, fundamenta la relevancia en los lineamientos de la política nacional de eficiencia administrativa al servicio del ciudadano y adopta el modelo de gestión pública eficiente, dirigido a mejorar la calidad de la gestión, como presentación de los servicios provistos por las entidades de la administración pública. Es de mencionar que el Plan Estratégico de tecnologías de la información (PETI)<sup>37</sup>, es aplicable tanto para entidades del estado como para el sector privado, por lo cual estos lineamientos hacen parte de una estructura diagnóstica que permite reconocer la importancia y la relevancia de la aplicación de los parámetros normativos aplicables a la gestión y control que pueden ser objetivamente direccionados desde la alta gerencia, por tanto, el ejercicio normativo internacional y la adopción de políticas nacionales aportan de manera significativa al desarrollo de los procesos que intervienen dinámicamente en los modelos que se deben adoptar en el marco de la protección de la infraestructura digital como un factor importante y transversal del cual hace parte la seguridad informática.

---

<sup>36</sup> CONPES 2013. Consejo Nacional de Política Económica y Social. DNP [página web]. (2, enero, 2013). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://colaboracion.dnp.gov.co/CDT/Normograma/CONPES%203785%20de%202013.pdf>>.

<sup>37</sup> MINTIC. G.ES.06 Guía para la construcción del PETI - Arquitectura TI. Mintic [página web]. (2, enero, 2020). [Consultado el 30, marzo, 2023]. Disponible en Internet: <<https://www.mintic.gov.co/arquitecturati/630/w3-article-15031.html>>.

## **5. DESARROLLO DE LOS OBJETIVOS**

A continuación, se desarrollan cada uno de los objetivos propuestos en el estudio, con el propósito de establecer los elementos que permiten la cohesión con respecto al análisis de las brechas de seguridad en infraestructura de TI en las entidades territoriales de sexta categoría (Alcaldía) en el territorio colombiano mediante consulta de fuentes especializadas con el fin de proponer recomendaciones y buenas prácticas que permitan gestionar el riesgo.

### **5.1. BRECHAS DE SEGURIDAD DE LOS ENTES TERRITORIALES ESPECÍFICAMENTE ALCALDÍAS**

Las brechas de seguridad digital son uno de los desafíos más apremiantes en la era de la información y la tecnología. Estas brechas representan vulnerabilidades o debilidades en la seguridad de sistemas, redes, aplicaciones o datos digitales que pueden ser explotadas por actores maliciosos con el fin de acceder, robar, dañar o comprometer información sensible o recursos críticos. A medida que la sociedad se vuelve cada vez más dependiente de la tecnología y la conectividad digital, las brechas de seguridad digital se han convertido en una preocupación para las entidades estatales .

#### **5.1.1. Brechas de seguridad**

El Gobierno Nacional publica para comentarios el documento borrador del decreto de ciberseguridad, que tiene por objeto : "Reglamentar parcialmente los artículos 147 y 230 de la Ley 1450 de 2011, modificado por el artículo 148 de la Ley 1955 de 2019 y el artículo 64 de la Ley 1437 de 2011, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital"<sup>38</sup>.

---

<sup>38</sup> MINTIC. Gobierno nacional publica borrador del decreto de ciberseguridad para el país - Gobierno nacional publica borrador del decreto de ciberseguridad para el país. MINTIC Colombia [página web]. (2022). [Consultado el 17, abril, 2023]. Disponible en Internet: <<https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/198588:Gobierno-nacional-publica-borrador-del-decreto-de-ciberseguridad-para-el-pais>>.

Los aspectos de involucran el manejo de las incidencias en Colombia se analizan en cuatros dimensiones específicamente, la gobernanza de la seguridad digital, la gestión del riesgo de la seguridad digital, la identificación de Infraestructuras Críticas y los incidentes de seguridad digital en el gobierno de Colombia. Por lo cual estos aspectos hacen parte los temas tratados por el Comité Nacional de Seguridad Digital, el cual se fundamenta con las acciones de emergencia que son atendidas por el ColCERT, Csirt del Gobierno de Colombia y Csirt de defensa.

Los ataques digitales en el estado colombiano, al igual que en otros países, son una preocupación creciente debido al aumento de la dependencia de la tecnología y la conectividad en la administración pública. Estos ataques pueden tomar diversas formas y tienen diversos objetivos. Algunos ejemplos de ataques digitales que pueden afectar al estado colombiano incluyen:

- Ciberataques: Estos ataques buscan comprometer la seguridad de los sistemas informáticos del gobierno colombiano. Pueden incluir ataques de denegación de servicio (DDoS), malware, ransomware y vulnerabilidades de software.
- Phishing: Los ataques de phishing son intentos de engañar a los funcionarios gubernamentales para que revelen información confidencial, como contraseñas o datos personales, a través de correos electrónicos falsos o sitios web fraudulentos.
- Ataques a la infraestructura crítica: Los atacantes pueden dirigirse a la infraestructura crítica del estado colombiano, como sistemas de energía, agua, comunicaciones o transporte, con el objetivo de interrumpir sus operaciones.
- Robo de datos: Los atacantes pueden buscar acceder y robar datos sensibles o confidenciales del gobierno, lo que puede tener graves implicaciones para la seguridad nacional y la privacidad de los ciudadanos.
- Desinformación y manipulación: Los actores maliciosos pueden difundir información falsa o manipulada en línea con el objetivo de influir en la opinión pública, socavar la confianza en el gobierno o desestabilizar el país.

Para hacer frente a estos desafíos, el gobierno colombiano debe tomar medidas para fortalecer su ciberseguridad, promover la conciencia sobre la seguridad digital entre sus funcionarios y ciudadanos, y establecer protocolos de respuesta a incidentes cibernéticos. También puede ser importante colaborar a nivel

internacional para identificar y perseguir a los actores detrás de estos ataques, ya que muchas veces operan desde fuera de las fronteras de Colombia.

#### **5.1.2. Posibles eventos de vulnerabilidad.**

Las actividades de las entidades territoriales de sexta categoría, desafortunadamente cuenta con procesos de inversión limitados, así como la asignación de presupuesto para el desarrollo de procesos y procedimientos acordes con el crecimiento de las tendencias de ciberseguridad que se deben tener presente para tales fines, elementos cotidianos en los procesos de automatización de copias de seguridad, procesos que involucran transferencia de datos seguros por medio de elementos como Redes Virtuales Privadas, configuración y manejo de Firewall, así como los correspondientes a la infraestructuras de red; hacen parte de fundamental del cumplimiento de las normatividad en cuanto al uso y privacidad de la información, y la seguridad de la misma.

Por lo anterior es importante reconocer que las entidades estatales deben establecer lineamientos de competencia en el desarrollo de modelos de ciberseguridad que se ajusten a las necesidades y por ende a la capacidad instalada con que cuenta la institución, no obstante estos elementos de control debe ser orientados con un personal idóneo en el desarrollo de estos procesos de aplicación y ejecución, desde la acción administrativa de la planeación, hasta el desarrollo de tareas que permitan el proceso afectivo de los lineamientos que aporten a la seguridad digital de las instituciones en caso de las Alcaldías de sexta categoría en el todo el territorio colombiano.

Por tanto los eventos posibles en los cuales se ven inmersas este tipo de entidades, tiene un factor común denominado Ingeniería Social, una metodología de ataque muy común por acceder a los correos electrónicos institucionales, por medio de mensajes de inmediates y urgencia, configurando una acción de respuesta psicológica a un evento inminente de riesgo, por ejemplo una notificación judicial, una acción de tutela, entre otros elementos similares que causan un evento de estrés en el usuario motivándolo a realizar acciones de apertura de correos no deseados y con contenido malicioso que finalmente termina por captar información de las instituciones con fines generalmente delincuenciales. Por lo cual es muy importante fortalecer los procesos de capacitación constante en los concerniente a

seguridad digital desde el usuario como estos también se convierten en un eslabón frágil de la cadena de protección de información .

De acuerdo con fuentes oficiales como ColCert , hacen parte las Vulnerabilidad Crítica en Microsoft (CVE-2024-38226), donde las macros de los aplicativos office pueden generar riesgos de vulnerabilidad, generalmente son ejecutados en las diferentes áreas de las organización por desconocimiento en los procesos, siendo uno de los factores de vulnerabilidad más comunes los que correspondiente en la recepción de correos electrónicos con elementos considerados maliciosos, otro de los elementos comunes, los que hacen referencia a las extensiones “SVG” (Gráficos de Vectores Escalables o Dimensionales) en los correos electrónicos institucionales; este tipo archivo es considerado sospechoso, cuando se remite como un archivo tipo documento y puede alojar un bot al ejecutarse, adicionalmente es una vulnerabilidad coincidente con el registro de base de datos internacional MITRE.

Las brechas de vulnerabilidad reflejan la importancia de mantener actualizados los sistemas y configurar adecuadamente las medidas de seguridad. La falta de actualización de software, combinada con configuraciones inadecuadas, abre la puerta a la explotación de vulnerabilidades críticas que podrían tener graves consecuencias en términos de pérdida de datos, interrupciones operativas y daños financieros.

Eventos críticos en las configuraciones red institucionales, los elementos conocidos como “cascadas”, hacen parte de una practica inadecuada en los procesos de infraestructura de red, donde lo ideal es la aplicación de puntos certificados para el desarrollo adecuado de los procesos de conectividad; si bien es una realidad en las alcaldías de categoría sexta en el territorio nacional, la poca disponibilidad presupuestal para implementar sistemas más seguros, se pueden optar por elementos de protección perimetral, como equipos con SO Mikrotik que permiten configuraciones adecuadas para el desarrollo de la protección de la red, desde el Firewall y las configuraciones propias contra ataques DDos y Permitir Acceso al RB por Winbox, web, ssh, telnet entre otros servicios, limitando solo a los administradores de red, así mismo generar protocolos de bloqueo a los puertos DNS desde la WAN, también generar el Bloqueo del puerto WebProxy desde la WAN lo cual es útil para proteger sus ips públicas por riesgo a hacer baneadas en lista negra, y por ultimo dentro de un parámetro estándar permitir acceso a internet solo a IPs autorizadas, por el administrador.

Lo anterior permite tener un control en el tráfico de datos de las instituciones fortaleciendo los controles, lo cual se puede sumar en la implementación de firewalls como Pfsense en dichos entornos de red.

### **5.1.3. Modelos análisis de riesgo.**

**5.1.3.1. ISO 27001: 2022.** Dentro de las acciones que comprenden las normas internacionales en el marco de trabajo de los Sistemas de Gestión de Seguridad de la Información SGSI, es importante establecer pilares como la confidencialidad, la integridad y la disponibilidad. Ya que las ISO 27001, aporta información relevante para realizar un ejercicio de gestión objetivo en el desarrollo de los procesos corporativos concernientes a la protección de datos privados y reservados, por lo cual alcanza relevancia en la medida que permite establecer controles para operar y mantener los procesos de los Sistemas de Gestión de Seguridad de la Información SGSI. En este orden la aplicación de dichos controles en la entidad públicas de sexta categoría, pueden adoptar parámetros de gestión que pueden aportar de manera significativa a la gestión institucional, en este caso de las alcaldías de categoría sexta.<sup>39</sup>

### **5.1.4. Gestión de activos de información.**

**5.1.4.1. Definición.** Los activos de información hacen parte fundamental de los datos que conforman las actividades cotidianas de los funcionarios en el desarrollo propios del ejercicio laboral. Dentro los activos se determinan las características del activo (tipo de dato, relevancia, ruta de almacenamiento, alojamiento, encriptación (si aplica), disponibilidad, duplicidad y accesos compartidos. En el ejercicio de valoración del activo se tienen presente (confidencialidad, integridad y disponibilidad) .

**5.1.4.2. Revisión.** La revisión de los activos se realiza de manera periódica, en tiempo de frecuencia temporal no mayores a 30 días, donde se genere un

---

<sup>39</sup> ISO27001. NQA Certification Body. NQA Global Accredited Certification Body [página web]. (2022). [Consultado el 6, mayo, 2024]. Disponible en Internet: <<https://www.nqa.com/es-co/certification/standards/iso-27001-2022#:~:text=¿Qué%20es%20la%20ISO%2027001,información,%20así%20como%20cumplimiento%20legal.>>>.

reporte de los procesos de seguridad de la información. Validando de esta forma el estado del activo.

**5.1.4.3. Gestión de control.** Los recursos digitales y medios de acceso serán validados por medio de contraseña segura en tanto para recursos web como para los locales y restricción de acceso a la red; solo generado rutas compartidas entre los equipos de trabajo directos, minimizando de esta forma el acceso y modificación de los datos, proporcionado un adecuado entorno de habilitación de los recursos compartidos en la red local. En el caso de los recursos compartidos en nube, se establecerán jerarquía en el ejercicio de acceso compartido, es decir la alta gerencia, hacen parte de los actores que intervienen el proceso de gestión y administración de la información. estandarización de los procedimientos de contraseñas seguras, manteniendo así la integridad, confidencialidad y disponibilidad de la información .

Es importante destacar que la ciberseguridad es un desafío global y en constante evolución, por lo que la protección de las infraestructuras digitales del estado colombiano debe ser una prioridad constante para garantizar la seguridad y el funcionamiento eficiente de las instituciones gubernamentales.

## **5.2. ANTECEDENTES, DE EVENTOS DE VULNERABILIDADES PRESENTADOS EN LAS ENTIDADES DE ORDEN TERRITORIAL DE CATEGORÍA SEXTA, ESPECÍFICAMENTE ALCALDÍAS**

Los ataques digitales que se han reportado en comparación con el año 2022, se observó una disminución de aproximadamente mil intentos de intrusión, ya que se registraron 6.300 millones de intentos en total. Esto marcó un aumento del 70 por ciento en comparación con el mismo período de 2021, que había tenido 3 mil millones de intentos.

Durante la primera mitad de 2023, América Latina y el Caribe experimentaron más de 63 mil millones de intentos de ciberataques. Brasil fue el país que recibió la mayor cantidad de estos intentos, con 23 mil millones, seguido de México con 14 mil millones, Venezuela con 10 mil millones, Colombia con 5 mil millones y Chile con 4 mil millones.

La compañía está preocupada por varias tendencias identificadas, especialmente la sofisticación de los ataques, ya que las organizaciones siguen siendo reactivas y se ha observado un aumento en el número de actores maliciosos involucrados.

A medida que los ataques de ransomware se vuelven más específicos, ha surgido la adopción de ransomware como servicio (RaaS). Sin embargo, FortiGuard Labs descubrió que hubo menos detecciones de ransomware en la primera mitad de 2023. A pesar de esta disminución general, se enfatiza la importancia de que las organizaciones mantengan su nivel de seguridad elevado, ya que la tendencia apunta a ataques cada vez más específicos .

En la primera mitad del año, se identificaron más de 10.000 vulnerabilidades únicas, lo que representa un aumento del 68 por ciento en comparación con cinco años atrás. Este aumento en la detección de exploits únicos resalta la diversidad de ataques maliciosos que los equipos de seguridad deben considerar.

El informe también señala una disminución del 75% en la cantidad de intentos de explotación por organización, lo que sugiere que, aunque hay más variantes de explotación, los ataques son ahora mucho más dirigidos que hace cinco años.

Por otro lado, los wipers, que son utilizados por actores de estados-naciones y están relacionados en gran medida con el conflicto entre Rusia y Ucrania, continúan siendo adoptados por grupos de ciberdelincuentes que apuntan a organizaciones en sectores como tecnología, manufactura, gobierno, telecomunicaciones y salud.

Un hallazgo adicional revela que las redes de bots ahora permanecen en línea durante períodos más prolongados que nunca. En los primeros seis meses de 2023, el tiempo promedio que estas redes de bots permanecieron en línea antes de que se cortaran las comunicaciones de comando y control (C2) fue de 83 días, lo que representa un aumento de más de 1.000 veces en comparación con cinco años atrás .

## **Ataque 01**

Ataque de cibernéticos en el ejercicio de las entidades públicas, registrados por el CSIRT Plataforma tecnológica que brinda servicios de nacionalización de alimentos y medicinas comprometida al parecer con un ransomware. El portal web fue deshabilitado y se desconectaron sus servidores físicos y virtuales. Además, el Invima indicó que la protección de la información, privacidad y confidencialidad de los datos que ellos manejan estaba asegurada por el acompañamiento del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) y las medidas implementadas por la propia entidad. Adicionalmente se advirtió una campaña de engaños con envíos de correos desde el dominio oficial de la entidad: [invima.gov.co](mailto:invima.gov.co)

## **Ataque 02**

Plataforma informática del Invima fue nuevamente objeto de un ataque cibernético. En consecuencia, se produjo la no disponibilidad de información y de los aplicativos externos, a excepción de la Ventanilla Única de Comercio Exterior (VUCE). El equipo técnico del Invima atendió este incidente, aunque aseguró que la información, privacidad y seguridad de los datos bajo su cargo se encontraban protegidos. Cabe anotar que se deshabilitó el portal web [invima.gov.co](http://invima.gov.co) y las conexiones con los servidores físicos y virtuales hasta que se controló la situación. Este segundo ataque incluyó una amenaza directa al director del instituto, en la que se habla de un plazo máximo de 3 días para contactar a los hackers o de lo contrario, “los 700 GB de datos confidenciales robados serán vendidos”, lo que denota nuevamente un ransomware

“Por lo anterior es importante realizar un seguimiento a los eventos que presentan en el país, específicamente en las entidades del estado como los entes territoriales como las alcaldías, esto en la medida, generar herramientas de prevención, y fortalecer las acciones de control que estas instituciones puedan aplicar para ejecutar lineamientos de control funcionales para el manejo de vulnerabilidades”.

### **5.3. MODELO DE ANÁLISIS Y GESTIÓN DEL RIESGO BASADO EN LAS CARACTERÍSTICAS DE INFRAESTRUCTURA TI**

Modelo de análisis y gestión del riesgo basado en las características de infraestructura TI de una entidad de sexta categoría, específicamente alcaldías

### **5.3.1. Objetivo**

El objetivo de este modelo es identificar los activos de información críticos que se afectarían la continuidad de una alcaldía, a partir de un análisis de los riesgos que pueden afectar su infraestructura TI.

### **5.3.2. Metodología**

El modelo se basa en los siguientes pasos:

**5.3.2.1. Identificación de los activos de información críticos.** En este paso se identifican los activos de información que son esenciales para el funcionamiento de la alcaldía. Estos activos pueden ser datos, sistemas, aplicaciones, infraestructura, entre otros.

**5.3.2.2. Evaluación de los riesgos.** En este paso se evalúan los riesgos que pueden afectar los activos de información identificados. Los riesgos pueden ser de origen natural, tecnológico, humano, entre otros.

**5.3.2.3. Análisis de impacto.** En este paso se analiza el impacto que tendría la materialización de cada riesgo sobre los activos de información críticos.

**5.3.2.4. Priorización de los riesgos** En este paso se priorizan los riesgos de acuerdo con su impacto.

**5.3.2.5. Implementación de controles.** En este paso se implementan controles para mitigar los riesgos priorizados.

Características de la infraestructura TI de una alcaldía. Las alcaldías son entidades públicas que brindan servicios a la comunidad. Su infraestructura TI suele estar compuesta por los siguientes elementos:

- Sistemas informáticos para la gestión de procesos administrativos, financieros, etc.
- Aplicaciones web para la prestación de servicios a los ciudadanos.
- Infraestructura de red para la conexión de los sistemas y aplicaciones.
- Servicios de almacenamiento para la conservación de los datos.
- Servicios de seguridad para la protección de los sistemas y datos.

**5.3.2.6. Análisis de riesgos.** Los riesgos que pueden afectar la infraestructura TI de una alcaldía son los siguientes

- Riesgos naturales, como terremotos, inundaciones, entre otros.
- Riesgos tecnológicos, como fallas en el hardware, software, entre otros.
- Riesgos humanos, como errores, fraudes, entre otros.
- Riesgos externos, como ataques cibernéticos, entre otros.
- Impacto de los riesgos

**5.3.2.7. El impacto de la materialización de un riesgo sobre los activos de información críticos puede ser el siguiente:**

- Pérdida de datos
- Inaccesibilidad a los sistemas
- Disrupción de los servicios
- Reputación dañada
- Priorización de los riesgos

**5.3.2.8. Los riesgos se pueden priorizar de acuerdo con los siguientes criterios:**

- Probabilidad de ocurrencia
- Impacto
- Costo de mitigación
- Controles

**5.3.2.9. Los controles son medidas que se implementan para mitigar los riesgos. Los controles pueden ser de los siguientes tipos:**

- Preventivos, que buscan evitar la ocurrencia de un riesgo.

- Detectivos, que buscan detectar la ocurrencia de un riesgo.
- Correctivos, que buscan mitigar el impacto de un riesgo .

Este modelo es una herramienta útil para identificar los activos de información críticos que se afectarían la continuidad de una alcaldía. El modelo se basa en un análisis de los riesgos que pueden afectar la infraestructura TI de la alcaldía.

Se recomienda que las alcaldías implementen este modelo para mejorar su gestión del riesgo. El modelo puede ayudar a las alcaldías a identificar los activos de información críticos y a implementar controles para mitigar los riesgos .

De acuerdo identificación de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAGERIT. Se deben reconocer los activos de información en una entidad, por lo cual se dispone un ejemplo con el propósito de reconocer los diferentes tipos de activos y las posibles amenazas que se pueden reconocer en el dicho ejercicio.<sup>40</sup>

Identificación de las amenazas de acuerdo a la metodología magerit, lo cual es importante par establece controles en el proceso de identificación de riesgos en los sistemas de información.

### **5.3.3. Tipos de Activos**

#### **5.3.3.1. Activos esenciales**

En un sistema de información hay 2 cosas esenciales: — la información que se maneja y — los servicios que prestan. Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema. Dentro de la información que se maneja, puede ser interesante considerar algunas características formales tales como si son de carácter personal, con requisitos legales, o si están sometidos a alguna clasificación de seguridad, con requisitos normativos:

---

<sup>40</sup> Dicho ejemplo no hace referencia acaso particular , solo se toman datos de referencia con el propósito de fortalecer el ejemplo de la tabla 1.

### Figura 1. Activos esenciales

```
[info] información
      [adm] datos de interés para la administración pública
      [vr] datos vitales (registros de la organización) (1)

      [per] datos de carácter personal (2)
            [A] nivel alto
            [M] nivel medio
            [B] nivel bajo

      [classified] datos clasificados (3)
            [C] nivel confidencial
            [R] difusión limitada
            [UC] sin clasificar
            [pub] de carácter público

[service] servicio
```

Fuente: Metodología magerit

### 5.3.3.2. Arquitectura de sistema.

#### Figura 2. Arquitectura de sistema

```
[sap] punto de [acceso al] servicio (1)

[ip] punto de interconexión (2)

[ext] proporcionado por terceros (3)
```

Fuente: Metodología magerit

### 5.3.3.3. Datos de información

#### Figura 3. Datos de información

```
[files] ficheros
[backup] copias de respaldo
[conf] datos de configuración (1)
[int] datos de gestión interna
[password] credenciales (ej. contraseñas)
[auth] datos de validación de credenciales
[acl] datos de control de acceso
[log] registro de actividad (2)
```

Fuente: Metodología magerit

#### 5.3.3.4. Claves criptográficas

**Figura 4. Claves criptográficas**

```
[info] protección de la información
  [encrypt] claves de cifra
    [shared_secret] secreto compartido (clave simétrica) (1)
    [public_encryption] clave pública de cifra (2)
    [public_decryption] clave privada de descifrado (2)
  [sign] claves de firma
    [shared_secret] secreto compartido (clave simétrica)
    [public_signature] clave privada de firma (2)
    [public_verification] clave pública de verificación de firma (2)

[com] protección de las comunicaciones
  [channel] claves de cifrado del canal
  [authentication] claves de autenticación
  [verification] claves de verificación de autenticación

[disk] cifrado de soportes de información
  [encrypt] claves de cifra

[x509] certificados de clave pública
```

Fuente: Metodología magerit

#### 5.3.3.5. Servicios

**Figura 5. Servicios**

```
[www] world wide web
[telnet] acceso remoto a cuenta local
[email] correo electrónico
[file] almacenamiento de ficheros
[ftp] transferencia de ficheros
[edi] intercambio electrónico de datos
[dir] servicio de directorio (1)
[idm] gestión de identidades (2)
[ipm] gestión de privilegios
[pki] PKI - infraestructura de clave pública (3)
```

Fuente: Metodología magerit

### 5.3.3.6. Software

**Figura 6. Software**

```
[prp] desarrollo propio (in house)
[sub] desarrollo a medida (subcontratado)
[std] estándar (off the shelf)
  [browser] navegador web
  [www] servidor de presentación
  [app] servidor de aplicaciones
  [email_client] cliente de correo electrónico
  [email_server] servidor de correo electrónico
  [file] servidor de ficheros
  [dbms] sistema de gestión de bases de datos
  [tm] monitor transaccional
  [office] ofimática
  [av] anti virus
  [os] sistema operativo
  [hypervisor] gestor de máquinas virtuales
  [ts] servidor de terminales
  [backup] sistema de backup
```

Fuente: Metodología magerit

### 5.3.3.7. Hardware

**Figura 7. Hardware**

```
[host] grandes equipos (1)
[mid] equipos medios (2)
[pc] informática personal (3)
[mobile] informática móvil (4)
[pda] agendas electrónicas
[vhost] equipo virtual
[backup] equipamiento de respaldo (5)
[peripheral] periféricos
  [print] medios de impresión (6)
  [scan] escáneres
  [crypto] dispositivos criptográficos
[bp] dispositivo de frontera (7)
[network] soporte de la red (8)
  [modem] módems
  [hub] concentradores
  [switch] conmutadores
  [router] encaminadores
  [bridge] pasarelas
  [firewall] cortafuegos
  [wap] punto de acceso inalámbrico
[pabx] centralita telefónica
[ipphone] teléfono IP
```

Fuente: Metodología magerit

### 5.3.3.8. Redes de comunicaciones

Figura 8. Redes de comunicación

```
[PSTN] red telefónica
[ISDN] rdsi (red digital)
[X25] X25 (red de datos)
[ADSL] ADSL
[pp] punto a punto
[radio] comunicaciones radio
[wifi] red inalámbrica
[mobile] telefonía móvil
[sat] por satélite
[LAN] red local
[MAN] red metropolitana
[Internet] Internet
```

Fuente: Metodología magerit

### 5.3.3.9. Soporte de información

Figura 9. Soporte de información

```
[electronic] electrónicos
  [disk] discos
  [vdisk] discos virtuales
  [san] almacenamiento en red
  [disquette] disquetes
  [cd] cederrón (CD-ROM)
  [usb] memorias USB
  [dvd] DVD
  [tape] cinta magnética
  [mc] tarjetas de memoria
  [ic] tarjetas inteligentes

[non_electronic] no electrónicos
  [printed] material impreso
  [tape] cinta de papel
  [film] microfilm
  [cards] tarjetas perforadas
```

Fuente: Metodología magerit

### 5.3.3.10. Equipamiento auxiliar

**Figura 10. Equipamiento auxiliar**

```
[power] fuentes de alimentación
[ups] sistemas de alimentación ininterrumpida
[gen] generadores eléctricos
[ac] equipos de climatización
[cabling] cableado
    [wire] cable eléctrico
    [fiber] fibra óptica
[robot] robots
    [tape] ... de cintas
    [disk] ... de discos
[supply] suministros esenciales
[destroy] equipos de destrucción de soportes de información
[furniture] mobiliario: armarios, etc
[safe] cajas fuertes
```

Fuente: Metodología magerit

### 5.3.3.11. Instalaciones

**Figura 11. Instalaciones**

```
[site] recinto
[building] edificio
[local] cuarto
[mobile] plataformas móviles
    [car] vehículo terrestre: coche, camión, etc.
    [plane] vehículo aéreo: avión, etc.
    [ship] vehículo marítimo: buque, lancha, etc.
    [shelter] contenedores
[channel] canalización
[backup] instalaciones de respaldo
```

Fuente: Metodología magerit

### 5.3.3.12. Personal

**Figura 12. Personal**

```
[ue] usuarios externos
[ui] usuarios internos
[op] operadores
[adm] administradores de sistemas
[com] administradores de comunicaciones
[dba] administradores de BBDD
[sec] administradores de seguridad
[des] desarrolladores / programadores
[sub] subcontratas
[prov] proveedores
```

---

Fuente: Metodología magerit

### 5.3.4. Amenazas

Tabla 1. Amenazas

| [código] descripción sucinta de lo que puede pasar                                                                                                       |                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"><li>• que se pueden ver afectados por este tipo de amenazas</li></ul>                         | <b>Dimensiones:</b> <ol style="list-style-type: none"><li>1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante</li></ol> |
| <b>Descripción:</b><br>complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas |                                                                                                                                                                              |

Fuente: Metodología magerit

#### 5.3.4.1. Desastres naturales

Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

Tabla 2. Fuego

| [N.1] Fuego                                                                                                                                                                                                                 |                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"><li>• [HW] equipos informáticos (hardware)</li><li>• [Media] soportes de información</li><li>• [AUX] equipamiento auxiliar</li><li>• [L] instalaciones</li></ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"><li>1. [D] disponibilidad</li></ol> |
| <b>Descripción:</b><br>incendios: posibilidad de que el fuego acabe con recursos del sistema.<br><b>Ver:</b><br>EBIOS: 01- INCENDIO                                                                                         |                                                                                           |

Fuente: Metodología magerit

Tabla 3. Daños por agua

| [N.2] Daños por agua                                                                                                                                                                                                        |                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"><li>• [HW] equipos informáticos (hardware)</li><li>• [Media] soportes de información</li><li>• [AUX] equipamiento auxiliar</li><li>• [L] instalaciones</li></ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"><li>1. [D] disponibilidad</li></ol> |
| <b>Descripción:</b><br>inundaciones: posibilidad de que el agua acabe con recursos del sistema.<br><b>Ver:</b><br>EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA                                                            |                                                                                           |

Fuente: Metodología magerit

**Tabla 4. Desastres naturales**

| <b>[N.*] Desastres naturales</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> <li>• [L] instalaciones</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>Dimensiones:</b><br>1. [D] disponibilidad |
| <b>Descripción:</b><br>otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, ...<br>Se excluyen desastres específicos tales como incendios (ver [N.1]) e inundaciones (ver [N.2]).<br>Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.<br><b>Ver:</b><br>EBIOS:<br>03 – CONTAMINACIÓN<br>04 - SINIESTRO MAYOR<br>06 - FENÓMENO CLIMÁTICO<br>07 - FENÓMENO SÍSMICO<br>08 - FENÓMENO DE ORIGEN VOLCÁNICO<br>09 - FENÓMENO METEOROLÓGICO<br>10 - INUNDACIÓN |                                              |

Fuente: Metodología magerit

### 5.3.4.2. Origen industrial

**Tabla 5. Origen industrial**

| <b>[I.1] Fuego</b>                                                                                                                                                                                                               |                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> <li>• [L] instalaciones</li> </ul> | <b>Dimensiones:</b><br>1. [D] disponibilidad |
| <b>Descripción:</b><br>incendio: posibilidad de que el fuego acabe con los recursos del sistema.<br><b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)<br><b>Ver:</b><br>EBIOS: 01- INCENDIO             |                                              |

Fuente: Metodología magerit

**Tabla 6. Daños por agua.**

| <b>[I.2] Daños por agua</b>                                                                                                                                                                                                                                        |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> <li>• [L] instalaciones</li> </ul>                                   | <b>Dimensiones:</b><br>1. [D] disponibilidad |
| <b>Descripción:</b><br>escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.<br><b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)<br><b>Ver:</b><br>EBIOS: 02 - PERJUICIOS OCASIONADOS POR EL AGUA |                                              |

Fuente: Metodología magerit

**Tabla 7. Desastres naturales**

| <b>[I.*] Desastres industriales</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> <li>• [L] instalaciones</li> </ul>                                                                                                                                                                                                                                                     | <b>Dimensiones:</b><br>1. [D] disponibilidad |
| <b>Descripción:</b><br>otros desastres debidos a la actividad humana: explosiones, derrumbes, ...<br>contaminación química, ...<br>sobrecarga eléctrica, fluctuaciones eléctricas, ...<br>accidentes de tráfico, ...<br>Se excluyen amenazas específicas como incendio (ver [I.1]) e inundación (ver [I.2]).<br>Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas. |                                              |
| <b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)                                                                                                                                                                                                                                                                                                                                                                                                           |                                              |
| <b>Ver:</b><br>EBIOS: 04 - SINIESTRO MAYOR                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                              |

Fuente: Metodología magerit

**Tabla 8. Contaminación mecánica**

| <b>[I.3] Contaminación mecánica</b>                                                                                                                                                                 |                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> </ul> | <b>Dimensiones:</b><br>1. [D] disponibilidad |
| <b>Descripción:</b><br>vibraciones, polvo, suciedad, ...                                                                                                                                            |                                              |
| <b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)                                                                                                                          |                                              |
| <b>Ver:</b><br>EBIOS: 03 – CONTAMINACIÓN                                                                                                                                                            |                                              |

Fuente: Metodología magerit

**Tabla 9. Contaminación electromagnética**

| <b>[I.4] Contaminación electromagnética</b>                                                                                                                                                                        |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información (electrónicos)</li> <li>• [AUX] equipamiento auxiliar</li> </ul> | <b>Dimensiones:</b><br>1. [D] disponibilidad |
| <b>Descripción:</b><br>interferencias de radio, campos magnéticos, luz ultravioleta, ...                                                                                                                           |                                              |
| <b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)                                                                                                                                         |                                              |
| <b>Ver:</b><br>EBIOS:<br>14 - EMISIONES ELECTROMAGNÉTICAS<br>15- RADIACIONES TÉRMICAS<br>16 - IMPULSOS ELECTROMAGNÉTICOS                                                                                           |                                              |

Fuente: Metodología magerit

**Tabla 10. Avería de origen físico o lógico**

| <b>[I.5] Avería de origen físico o lógico</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [SW] aplicaciones (software)</li> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> </ul>                                                                                                                                                                                                                                                                                                            | <b>Dimensiones:</b><br>1. [D] disponibilidad |
| <b>Descripción:</b><br>fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.<br>En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.<br><b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)<br><b>Ver:</b><br>EBIOS:<br>28 - AVERÍA DEL HARDWARE<br>29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE |                                              |

Fuente: Metodología magerit

**Tabla 11. Corte del suministro eléctrico**

| <b>[I.6] Corte del suministro eléctrico</b>                                                                                                                                                                        |                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información (electrónicos)</li> <li>• [AUX] equipamiento auxiliar</li> </ul> | <b>Dimensiones:</b><br>1. [D] disponibilidad |
| <b>Descripción:</b><br>cese de la alimentación de potencia<br><b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)<br><b>Ver:</b><br>EBIOS: 12 - PÉRDIDA DE SUMINISTRO DE ENERGÍA            |                                              |

Fuente: Metodología magerit

**Tabla 12. Condiciones inadecuadas de temperatura**

| <b>[I.7] Condiciones inadecuadas de temperatura y/o humedad</b>                                                                                                                                                                                                                                                       |                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> </ul>                                                                                                                   | <b>Dimensiones:</b><br>1. [D] disponibilidad |
| <b>Descripción:</b><br>deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, ...<br><b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)<br><b>Ver:</b><br>EBIOS: 11- FALLAS EN LA CLIMATIZACIÓN |                                              |

Fuente: Metodología magerit

**Tabla 13. Fallo de servicios de comunicaciones**

| <b>[I.8] Fallo de servicios de comunicaciones</b>                                                                                                                                                                                                                                                         |                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <b>Tipos de activos:</b>                                                                                                                                                                                                                                                                                  | <b>Dimensiones:</b>   |
| <ul style="list-style-type: none"> <li>[COM] redes de comunicaciones</li> </ul>                                                                                                                                                                                                                           | 1. [D] disponibilidad |
| <b>Descripción:</b><br>cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente. |                       |
| <b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)                                                                                                                                                                                                                                |                       |
| <b>Ver:</b><br>EBIOS: 13 - PÉRDIDA DE LOS MEDIOS DE TELECOMUNICACIÓN                                                                                                                                                                                                                                      |                       |

Fuente: Metodología magerit

**Tabla 14. Interrupción de otros servicios y suministros esenciales**

| <b>[I.9] Interrupción de otros servicios y suministros esenciales</b>                                                                                              |                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <b>Tipos de activos:</b>                                                                                                                                           | <b>Dimensiones:</b>   |
| <ul style="list-style-type: none"> <li>[AUX] equipamiento auxiliar</li> </ul>                                                                                      | 1. [D] disponibilidad |
| <b>Descripción:</b><br>otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, toner, refrigerante, ... |                       |
| <b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)                                                                                         |                       |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                                                                |                       |

Fuente: Metodología magerit

**Tabla 15. Degradación de los soportes de almacenamiento de la información**

| <b>[I.10] Degradación de los soportes de almacenamiento de la información</b>                  |                       |
|------------------------------------------------------------------------------------------------|-----------------------|
| <b>Tipos de activos:</b>                                                                       | <b>Dimensiones:</b>   |
| <ul style="list-style-type: none"> <li>[Media] soportes de información</li> </ul>              | 1. [D] disponibilidad |
| <b>Descripción:</b><br>como consecuencia del paso del tiempo                                   |                       |
| <b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)                     |                       |
| <b>Ver:</b><br>EBIOS:<br>28 - AVERÍA DEL HARDWARE<br>29 - FALLA DE FUNCIONAMIENTO DEL HARDWARE |                       |

Fuente: Metodología magerit

**Tabla 16. Emanaciones electromagnéticas**

| <b>[I.11] Emanaciones electromagnéticas</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] media</li> <li>• [AUX] equipamiento auxiliar</li> <li>• [L] instalaciones</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque.<br><br>Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información.<br><br>Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés " <i>Transient Electromagnetic Pulse Standard</i> "). Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de " <i>TEMPEST protection</i> ", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara.<br><br>No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.<br><br><b>Origen:</b><br>Entorno (accidental)<br>Humano (accidental o deliberado)<br><br><b>Ver:</b><br>EBIOS: 17 - INTERCEPTACIÓN DE SEÑALES PARÁSITAS COMPROMETEDORAS |                                                                                               |

Fuente: Metodología magerit

#### **5.3.4.3. Errores y Fallos no intencionados**

Fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados, muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto. Este tipo de fallos esta relacionado con el factor humano.

**Tabla 17. Errores de los usuarios**

| <b>[E.1] Errores de los usuarios</b>                                                                                                                                                                                                                     |                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [D] datos / información</li> <li>• [keys] claves criptográficas</li> <li>• [S] servicios</li> <li>• [SW] aplicaciones (software)</li> <li>• [Media] soportes de información</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [I] integridad</li> <li>2. [C] confidencialidad</li> <li>3. [D] disponibilidad</li> </ol> |
| <b>Descripción:</b><br>equivocaciones de las personas cuando usan los servicios, datos, etc.<br><b>Ver:</b><br>EBIOS: 38 - ERROR DE USO                                                                                                                  |                                                                                                                                                         |

Fuente: Metodología magerit

**Tabla 18. Errores del administrador**

| <b>[E.2] Errores del administrador</b>                                                                                                                                                                                                                                                                                                            |                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [D] datos / información</li> <li>• [keys] claves criptográficas</li> <li>• [S] servicios</li> <li>• [SW] aplicaciones (software)</li> <li>• [HW] equipos informáticos (hardware)</li> <li>• [COM] redes de comunicaciones</li> <li>• [Media] soportes de información</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [D] disponibilidad</li> <li>2. [I] integridad</li> <li>3. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>equivocaciones de personas con responsabilidades de instalación y operación<br><b>Ver:</b><br>EBIOS: 38 - ERROR DE USO                                                                                                                                                                                                     |                                                                                                                                                         |

Fuente: Metodología magerit

**Tabla 19. Errores del monitorización**

| <b>[E.3] Errores de monitorización (log)</b>                                                                                                                                                                               |                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [D.log] registros de actividad</li> </ul>                                                                                                                | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [I] integridad (trazabilidad)</li> </ol> |
| <b>Descripción:</b><br>inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, ...<br><b>Ver:</b><br>EBIOS: no disponible |                                                                                                        |

Fuente: Metodología magerit

**Tabla 20. Errores de configuración**

| <b>[E.4] Errores de configuración</b>                                                                                                                                                                                                                                            |                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <b>Tipos de activos:</b>                                                                                                                                                                                                                                                         | <b>Dimensiones:</b> |
| <ul style="list-style-type: none"> <li>[D.conf] datos de configuración</li> </ul>                                                                                                                                                                                                | 1. [I] integridad   |
| <b>Descripción:</b><br>introducción de datos de configuración erróneos.<br><br>Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. |                     |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                                                                                                                                                                              |                     |

Fuente: Metodología magerit

**Tabla 21. Deficiencias en la organización**

| <b>[E.7] Deficiencias en la organización</b>                                                                                                                                                                                           |                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <b>Tipos de activos:</b>                                                                                                                                                                                                               | <b>Dimensiones:</b>   |
| <ul style="list-style-type: none"> <li>[P] personal</li> </ul>                                                                                                                                                                         | 1. [D] disponibilidad |
| <b>Descripción:</b><br>cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión.<br><br>Acciones descoordinadas, errores por omisión, etc. |                       |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                                                                                                                                    |                       |

Fuente: Metodología magerit

**Tabla 22. Difusión de software dañino**

| <b>[E.8] Difusión de software dañino</b>                                                                                 |                                                                       |
|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Tipos de activos:</b>                                                                                                 | <b>Dimensiones:</b>                                                   |
| <ul style="list-style-type: none"> <li>[SW] aplicaciones (software)</li> </ul>                                           | 1. [D] disponibilidad<br>2. [I] integridad<br>3. [C] confidencialidad |
| <b>Descripción:</b><br>propagación inocente de virus, espías ( <i>spyware</i> ), gusanos, troyanos, bombas lógicas, etc. |                                                                       |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                      |                                                                       |

Fuente: Metodología magerit

**Tabla 23. Errores de encaminamiento**

| <b>[E.9] Errores de [re-]encaminamiento</b>                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [S] servicios</li> <li>• [SW] aplicaciones (software)</li> <li>• [COM] redes de comunicaciones</li> </ul>                                                                                                                                                                                                                                                                                                         | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.<br><br>Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.<br><br><b>Ver:</b><br>EBIOS: no disponible |                                                                                               |

Fuente: Metodología magerit

**Tabla 24. Errores de secuencia**

| <b>[E.10] Errores de secuencia</b>                                                                                                                                          |                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [S] servicios</li> <li>• [SW] aplicaciones (software)</li> <li>• [COM] redes de comunicaciones</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [I] integridad</li> </ol> |
| <b>Descripción:</b><br>alteración accidental del orden de los mensajes transmitidos.<br><br><b>Ver:</b><br>EBIOS: no disponible                                             |                                                                                         |

Fuente: Metodología magerit

**Tabla 25. Escapes de información**

| <b>[E.14] Escapes de información</b>                                                                                                                                                    |                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>•</li> </ul>                                                                                                            | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada. |                                                                                               |

Fuente: Metodología magerit

**Tabla 26. Alteración accidental de la información**

| <b>[E.15] Alteración accidental de la información</b>                                                                                                                                                                                                                                                                      |                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [D] datos / información</li> <li>• [keys] claves criptográficas</li> <li>• [S] servicios</li> <li>• [SW] aplicaciones (SW)</li> <li>• [COM] comunicaciones (tránsito)</li> <li>• [Media] soportes de información</li> <li>• [L] instalaciones</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [I] integridad</li> </ol> |
| <b>Descripción:</b><br>alteración accidental de la información.<br>Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.<br><b>Ver:</b><br>EBIOS: no disponible                                                                  |                                                                                         |

Fuente: Metodología magerit

**Tabla 27. Destrucción de la información**

| <b>[E.18] Destrucción de información</b>                                                                                                                                                                                                                                                                                   |                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [D] datos / información</li> <li>• [keys] claves criptográficas</li> <li>• [S] servicios</li> <li>• [SW] aplicaciones (SW)</li> <li>• [COM] comunicaciones (tránsito)</li> <li>• [Media] soportes de información</li> <li>• [L] instalaciones</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [D] disponibilidad</li> </ol> |
| <b>Descripción:</b><br>pérdida accidental de información.<br>Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.<br><b>Ver:</b><br>EBIOS: no disponible                                                                        |                                                                                             |

Fuente: Metodología magerit

**Tabla 28. Fugas de información**

| <b>[E.19] Fugas de información</b>                                                                                                                                                                                                                                                                                                                              |                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [D] datos / información</li> <li>• [keys] claves criptográficas</li> <li>• [S] servicios</li> <li>• [SW] aplicaciones (SW)</li> <li>• [COM] comunicaciones (tránsito)</li> <li>• [Media] soportes de información</li> <li>• [L] instalaciones</li> <li>• [P] personal (revelación)</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>revelación por indiscreción.<br>Incontinencia verbal, medios electrónicos, soporte papel, etc.<br><b>Ver:</b><br>EBIOS: no disponible                                                                                                                                                                                                    |                                                                                               |

Fuente: Metodología magerit

**Tabla 29. Vulnerabilidades de los programas**

| <b>[E.20] Vulnerabilidades de los programas (software)</b>                                                                                                                                                      |                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>[SW] aplicaciones (software)</li> </ul>                                                                                                         | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>[I] integridad</li> <li>[D] disponibilidad</li> <li>[C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. |                                                                                                                                                |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                                                                                                             |                                                                                                                                                |

Fuente: Metodología magerit

**Tabla 30. Errores de mantenimiento**

| <b>[E.21] Errores de mantenimiento / actualización de programas (software)</b>                                                                                                                    |                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>[SW] aplicaciones (software)</li> </ul>                                                                                           | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>[I] integridad</li> <li>[D] disponibilidad</li> </ol> |
| <b>Descripción:</b><br>defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. |                                                                                                                  |
| <b>Ver:</b><br>EBIOS: <ol style="list-style-type: none"> <li>31 - FALLA DE FUNCIONAMIENTO DEL SOFTWARE</li> <li>32 - PERJUICIO A LA MANTENIBILIDAD DEL SISTEMA DE INFORMACIÓN</li> </ol>          |                                                                                                                  |

Fuente: Metodología magerit

**Tabla 31. Caída del sistema por agotamiento de recursos**

| <b>[E.24] Caída del sistema por agotamiento de recursos</b>                                                                                                                   |                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>[S] servicios</li> <li>[HW] equipos informáticos (hardware)</li> <li>[COM] redes de comunicaciones</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>[D] disponibilidad</li> </ol> |
| <b>Descripción:</b><br>la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.                                            |                                                                                          |
| <b>Ver:</b><br>EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO                                                                                                                 |                                                                                          |

Fuente: Metodología magerit

**Tabla 32. Robo**

| <b>[E.25] Robo</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> </ul>                                                                                                                                                                                                                                                               | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [D] disponibilidad</li> <li>2. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.<br><br>Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales.<br><br>En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.<br><b>Ver:</b><br>EBIOS: 22 - RECUPERACIÓN DE SOPORTES RECICLADOS O DESECHADOS |                                                                                                                              |

Fuente: Metodología magerit

#### **5.3.4.4. Ataques Intencionados**

Fallos deliberados causados por las personas.

La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto. Estos eventos están relacionados con el factor humano.

**Tabla 33. Manipulación de los registros de actividad**

| <b>[A.4] Manipulación de los registros de actividad (log)</b>                                               |                                                                                                        |
|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [D.log] registros de actividad</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [I] integridad (trazabilidad)</li> </ol> |
| <b>Descripción:</b><br><br><b>Ver:</b><br>EBIOS: no disponible                                              |                                                                                                        |

Fuente: Metodología magerit

**Tabla 34. Manipulación de la configuración**

| <b>[A.4] Manipulación de la configuración</b>                                                                                                                                                                            |                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>[D.log] registros de actividad</li> </ul>                                                                                                                | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>[I] integridad</li> <li>[C] confidencialidad</li> <li>[A] disponibilidad</li> </ol> |
| <b>Descripción:</b><br>prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. |                                                                                                                                                |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                                                                                                                      |                                                                                                                                                |

Fuente: Metodología magerit

**Tabla 35. Suplantación de la identidad del usuario**

| <b>[A.5] Suplantación de la identidad del usuario</b>                                                                                                                                                                                                                                                 |                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>[D] datos / información</li> <li>[keys] claves criptográficas</li> <li>[S] servicios</li> <li>[SW] aplicaciones (software)</li> <li>[COM] redes de comunicaciones</li> </ul>                                                          | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>[C] confidencialidad</li> <li>[A] autenticidad</li> <li>[I] integridad</li> </ol> |
| <b>Descripción:</b><br>cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.<br><br>Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. |                                                                                                                                              |
| <b>Ver:</b><br>EBIOS: 40 - USURPACIÓN DE DERECHO                                                                                                                                                                                                                                                      |                                                                                                                                              |

**Tabla 36. Abusos de privilegios de acceso**

| <b>[A.6] Abuso de privilegios de acceso</b>                                                                                                                                                                                                                                                |                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>[D] datos / información</li> <li>[keys] claves criptográficas</li> <li>[S] servicios</li> <li>[SW] aplicaciones (software)</li> <li>[HW] equipos informáticos (hardware)</li> <li>[COM] redes de comunicaciones</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>[C] confidencialidad</li> <li>[I] integridad</li> <li>[D] disponibilidad</li> </ol> |
| <b>Descripción:</b><br>cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.                                                                |                                                                                                                                                |
| <b>Ver:</b><br>EBIOS: 39 - ABUSO DE DERECHO                                                                                                                                                                                                                                                |                                                                                                                                                |

Fuente: Metodología magerit

**Tabla 37. Uso no previsto**

| <b>[A.7] Uso no previsto</b>                                                                                                                                                                                                                                                                                                               |                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [S] servicios</li> <li>• [SW] aplicaciones (software)</li> <li>• [HW] equipos informáticos (hardware)</li> <li>• [COM] redes de comunicaciones</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> <li>• [L] instalaciones</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [D] disponibilidad</li> <li>2. [C] confidencialidad</li> <li>3. [I] integridad</li> </ol> |
| <b>Descripción:</b><br>utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.                                                                               |                                                                                                                                                         |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                                                                                                                                                                                                                                        |                                                                                                                                                         |

Fuente: Metodología magerit

**Tabla 38. Difusión de software dañino**

| <b>[A.8] Difusión de software dañino</b>                                                                                     |                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [SW] aplicaciones (software)</li> </ul>                    | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [D] disponibilidad</li> <li>2. [I] integridad</li> <li>3. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>propagación intencionada de virus, espías ( <i>spyware</i> ), gusanos, troyanos, bombas lógicas, etc. |                                                                                                                                                         |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                          |                                                                                                                                                         |

Fuente: Metodología magerit

**Tabla 39. Re encaminamiento de mensajes**

| <b>[A.9] [Re-]encaminamiento de mensajes</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [S] servicios</li> <li>• [SW] aplicaciones (software)</li> <li>• [COM] redes de comunicaciones</li> </ul>                                                                                                                                                                                                                                                                                                                                                                            | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros.<br><br>Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado.<br><br>Es particularmente destacable el caso de que el ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe. |                                                                                               |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                               |

Fuente: Metodología magerit

**Tabla 40. Alteración de secuencia**

| <b>[A.10] Alteración de secuencia</b>                                                                                                                                                                          |                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [S] servicios</li> <li>• [SW] aplicaciones (software)</li> <li>• [COM] redes de comunicaciones</li> </ul>                                    | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [I] integridad</li> </ol> |
| <b>Descripción:</b><br>alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados. |                                                                                         |
| <b>Ver:</b><br>EBIOS: 36 - ALTERACIÓN DE DATOS                                                                                                                                                                 |                                                                                         |

Fuente: Metodología magerit

**Tabla 41. Análisis de tráfico**

| <b>[A.12] Análisis de tráfico</b>                                                                                                                                                                                                                                                        |                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [COM] redes de comunicaciones</li> </ul>                                                                                                                                                                               | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>el atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.<br><br>A veces se denomina “monitorización de tráfico”. |                                                                                               |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                                                                                                                                                                                      |                                                                                               |

Fuente: Metodología magerit

**Tabla 42. Repudio**

| <b>[A.13] Repudio</b>                                                                                                                                                                                                                                                                                                                                            |                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [S] servicios</li> <li>• [D.log] registros de actividad</li> </ul>                                                                                                                                                                                                                             | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [I] integridad (trazabilidad)</li> </ol> |
| <b>Descripción:</b><br>negación a posteriori de actuaciones o compromisos adquiridos en el pasado.<br>Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación.<br>Repudio de recepción: negación de haber recibido un mensaje o comunicación.<br>Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro. |                                                                                                        |
| <b>Ver:</b><br>EBIOS: 41 - NEGACIÓN DE ACCIONES                                                                                                                                                                                                                                                                                                                  |                                                                                                        |

Fuente: Metodología magerit

**Tabla 43. Interceptación de información**

| <b>[A.14] Interceptación de información (escucha)</b>                                                                                            |                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [COM] redes de comunicaciones</li> </ul>                                       | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada. |                                                                                               |
| <b>Ver:</b><br>EBIOS: 19 - ESCUCHA PASIVA                                                                                                        |                                                                                               |

Fuente: Metodología magerit

**Tabla 44. Modificación deliberada de la información**

| <b>[A.15] Modificación deliberada de la información</b>                                                                                                                                                                                                                                                                             |                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [D] datos / información</li> <li>• [keys] claves criptográficas</li> <li>• [S] servicios (acceso)</li> <li>• [SW] aplicaciones (SW)</li> <li>• [COM] comunicaciones (tránsito)</li> <li>• [Media] soportes de información</li> <li>• [L] instalaciones</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [I] integridad</li> </ol> |
| <b>Descripción:</b><br>alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.                                                                                                                                                                                                           |                                                                                         |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                                                                                                                                                                                                                                 |                                                                                         |

Fuente: Metodología magerit

**Tabla 45. Destrucción de información**

| <b>[A.18] Destrucción de información</b>                                                                                                                                                                                                                                                 |                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [D] datos / información</li> <li>• [keys] claves criptográficas</li> <li>• [S] servicios (acceso)</li> <li>• [SW] aplicaciones (SW)</li> <li>• [Media] soportes de información</li> <li>• [L] instalaciones</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [D] disponibilidad</li> </ol> |
| <b>Descripción:</b><br>eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.                                                                                                                                                                  |                                                                                             |
| <b>Ver:</b><br>EBIOS: no disponible                                                                                                                                                                                                                                                      |                                                                                             |

Fuente: Metodología magerit

**Tabla 46. Revelación de información**

| <b>[A.19] Revelación de información</b>                                                                                                                                                                                                                                                                                             |                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [D] datos / información</li> <li>• [keys] claves criptográficas</li> <li>• [S] servicios (acceso)</li> <li>• [SW] aplicaciones (SW)</li> <li>• [COM] comunicaciones (tránsito)</li> <li>• [Media] soportes de información</li> <li>• [L] instalaciones</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>revelación de información.<br><b>Ver:</b><br>EBIOS: <ul style="list-style-type: none"> <li>23 – DIVULGACIÓN</li> <li>27 – GEOLOCALIZACIÓN</li> <li>34 - COPIA ILEGAL DE SOFTWARE</li> </ul>                                                                                                                  |                                                                                               |

Fuente: Metodología magerit

**Tabla 47. Manipulación de programas**

| <b>[A.22] Manipulación de programas</b>                                                                                                                                                                                 |                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [SW] aplicaciones (software)</li> </ul>                                                                                                               | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [C] confidencialidad</li> <li>2. [I] integridad</li> <li>3. [D] disponibilidad</li> </ol> |
| <b>Descripción:</b><br>alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.<br><b>Ver:</b><br>EBIOS: 26 - ALTERACIÓN DE PROGRAMAS |                                                                                                                                                         |

Fuente: Metodología magerit

**Tabla 48. Manipulación de los equipos**

| <b>[A.22] Manipulación de los equipos</b>                                                                                                                                                                             |                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> </ul>                                           | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [C] confidencialidad</li> <li>2. [D] disponibilidad</li> </ol> |
| <b>Descripción:</b><br>alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.<br><b>Ver:</b><br>EBIOS: 25 - SABOTAJE DEL HARDWARE |                                                                                                                              |

Fuente: Metodología magerit

**Tabla 49. Denegación de servicio**

| <b>[A.24] Denegación de servicio</b>                                                                                                                                                |                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [S] servicios</li> <li>• [HW] equipos informáticos (hardware)</li> <li>• [COM] redes de comunicaciones</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [D] disponibilidad</li> </ol> |
| <b>Descripción:</b><br>la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.                                                  |                                                                                             |
| <b>Ver:</b><br>EBIOS: 30 - SATURACIÓN DEL SISTEMA INFORMÁTICO                                                                                                                       |                                                                                             |

Fuente: Metodología magerit

**Tabla 50. Robo**

| <b>[A.25] Robo</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>3. [D] disponibilidad</li> <li>4. [C] confidencialidad</li> </ol> |
| <b>Descripción:</b><br>la sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.<br><br>El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.<br><br>El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.<br><br>En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. |                                                                                                                              |
| <b>Ver:</b><br>EBIOS:<br>20 - ROBO DE SOPORTES O DOCUMENTOS<br>21 - ROBO DE HARDWARE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                              |

Fuente: Metodología magerit

**Tabla 51. Ataque destructivo**

| <b>[A.26] Ataque destructivo</b>                                                                                                                                                                                                 |                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Tipos de activos:</b> <ul style="list-style-type: none"> <li>• [HW] equipos informáticos (hardware)</li> <li>• [Media] soportes de información</li> <li>• [AUX] equipamiento auxiliar</li> <li>• [L] instalaciones</li> </ul> | <b>Dimensiones:</b> <ol style="list-style-type: none"> <li>1. [D] disponibilidad</li> </ol> |
| <b>Descripción:</b><br>vandalismo, terrorismo, acción militar, ...<br><br>Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.            |                                                                                             |
| <b>Ver:</b><br>EBIOS: 05 - DESTRUCCIÓN DE HARDWARE O DE SOPORTES                                                                                                                                                                 |                                                                                             |

Fuente: Metodología magerit

**Tabla 52. Indisponibilidad del personal**

| <b>[A.28] Indisponibilidad del personal</b>                                                                                                                                                                                |                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <b>Tipos de activos:</b>                                                                                                                                                                                                   | <b>Dimensiones:</b>   |
| <ul style="list-style-type: none"> <li>[P] personal interno</li> </ul>                                                                                                                                                     | 1. [D] disponibilidad |
| <b>Descripción:</b><br>ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, ...<br><b>Ver:</b><br>EBIOS: 42 - DAÑO A LA DISPONIBILIDAD DEL PERSONAL |                       |

Fuente: Metodología magerit

**Tabla 53. Extorsión**

| <b>[A.29] Extorsión</b>                                                                                                                                              |                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Tipos de activos:</b>                                                                                                                                             | <b>Dimensiones:</b>                                                   |
| <ul style="list-style-type: none"> <li>[P] personal interno</li> </ul>                                                                                               | 1. [C] confidencialidad<br>2. [I] integridad<br>3. [D] disponibilidad |
| <b>Descripción:</b><br>presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.<br><b>Ver:</b><br>EBIOS: no disponible |                                                                       |

Fuente: Metodología magerit

**Tabla 54. Ingeniería social**

| <b>[A.30] Ingeniería social (picaresca)</b>                                                                                                                  |                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Tipos de activos:</b>                                                                                                                                     | <b>Dimensiones:</b>                                                   |
| <ul style="list-style-type: none"> <li>[P] personal interno</li> </ul>                                                                                       | 1. [C] confidencialidad<br>2. [I] integridad<br>3. [D] disponibilidad |
| <b>Descripción:</b><br>abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.<br><b>Ver:</b><br>EBIOS: no disponible |                                                                       |

Fuente: Metodología magerit

### 5.3.5. Correlación de errores y ataques metodología magerit

Tabla 55. Correlación de errores y ataques metodología magerit

| número | error                                                            | ataque                                     |
|--------|------------------------------------------------------------------|--------------------------------------------|
| 1      | Errores de los usuarios                                          |                                            |
| 2      | Errores del administrador                                        |                                            |
| 3      | Errores de monitorización (log)                                  | Manipulación de los registros de actividad |
| 4      | Errores de configuración                                         | Manipulación de la configuración           |
| 5      | Suplantación de la identidad del usuario                         |                                            |
| 6      | Abuso de privilegios de acceso                                   |                                            |
| 7      | Deficiencias en la organización                                  | Uso no previsto                            |
| 8      | Difusión de software dañino                                      | Difusión de software dañino                |
| 9      | Errores de [re-]encaminamiento                                   | [Re-]encaminamiento de mensajes            |
| 10     | Errores de secuencia                                             | Alteración de secuencia                    |
| 11     | Acceso no autorizado                                             |                                            |
| 12     | Análisis de tráfico                                              |                                            |
| 13     | Repudio                                                          |                                            |
| 14     | Escapes de información                                           | Interceptación de información (escucha)    |
| 15     | Alteración accidental de la información                          | Modificación deliberada de la información  |
| 18     | Destrucción de información                                       | Destrucción de información                 |
| 19     | Fugas de información                                             | Revelación de información                  |
| 20     | Vulnerabilidades de los programas (software)                     |                                            |
| 21     | Errores de mantenimiento / actualización de programas (software) |                                            |
| 22     | Manipulación de programas                                        |                                            |
| 23     | Errores de mantenimiento / actualización de equipos (hardware)   | Manipulación de los equipos                |
| 24     | Caída del sistema por agotamiento de recursos                    | Denegación de servicio                     |
| 25     | Pérdida de equipos                                               | Robo                                       |
| 26     | Ataque destructivo                                               |                                            |
| 27     | Ocupación enemiga                                                |                                            |
| 28     | Indisponibilidad del personal                                    | Indisponibilidad del personal              |
| 29     | Extorsión                                                        |                                            |
| 30     | Ingeniería social (picaresca)                                    |                                            |

Fuente: Metodología magerit

**Tabla 56. Ejemplo de identificación de activos y riesgos del mismo.**

| NÚMERO | ACTIVO   | NOMBRE DEL ACTIVO                                 | AMENAZA 1                             | VULNERABILIDADES                                                                                                                                                                                                                       |
|--------|----------|---------------------------------------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1      | SOFTWARE | Oracle CRM                                        | [I5] Avería de origen físico o lógico | CVE-2022-21598 - Vulnerabilidad en el producto Siebel Core - DB Deployment and Configuration de Oracle Siebel CRM (componente: Repository Utilities). Las versiones compatibles que se ven afectadas son la 22.8 y anteriores.         |
| 2      | DATOS    | Política de copias de seguridad de la información | [E18] Destrucción de información      | CVE-2022-48324-Registro de multiples ataques relacionados con la perdida de información / CVE-2022-4514 Una vulnerabilidad fue encontrada en Opencaching Deutschland oc-server3 y clasificada como problemática.                       |
| 3      | DATOS    | Política de control de acceso                     | [E18] Destrucción de información      | CVE-2022-48324-Registro de multiples ataques relacionados con la perdida de información / CVE-2022-48324 Múltiples vulnerabilidades de Cross Site Scripting (XSS) en Mapos 4.39.0 permiten a los atacantes ejecutar código arbitrario. |
| 4      | DATOS    | Política de tratamiento de datos                  | [E18] Destrucción de información      | CVE-2022-48324-Registro de multiples ataques relacionados con la perdida de información / CVE-2022-48324 Múltiples vulnerabilidades de Cross Site Scripting (XSS) en Mapos 4.39.0 permiten a los atacantes ejecutar código arbitrario. |

Continuación...

| NÚMERO | ACTIVO         | NOMBRE DEL ACTIVO       | AMENAZA 1                            | VULNERABILIDADES                                                                                                                                                                                                                                                                                                                                                         |
|--------|----------------|-------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5      | CRIPTOGRÁFICAS | Política de contraseñas | [E18] Destrucción de información     | CVE-2022-3589 - Un punto final de API utilizado por la aplicación móvil "AppWash" de Miele en todas las versiones era vulnerable a una omisión de autorización. Un atacante remoto con pocos privilegios habría podido obtener acceso de lectura y escritura parcial a los datos de otros usuarios modificando una pequeña parte de una solicitud HTTP enviada a la API. |
| 6      | PERSONAL       | Director de TI          | [E7] Deficiencias en la organización | CVE-2023-27490 - Ataques relacionados con ingeniería social / CVE-2022-42785 Múltiples productos W&T de la serie ComServer son propensos a omitir la autenticación. Un atacante remoto no autenticado puede iniciar sesión sin conocer la contraseña mediante la elaboración de una solicitud HTTP GET modificada.                                                       |

Fuente: Elaboración propia

Por lo anterior se fundamenta cada una de las acciones que corresponde el proceso de identificación de los activos para para el abordaje de una matriz de riesgo, siendo importante el reconocimiento de las vulnerabilidades que pueden afectar cada uno de estos y las políticas que lo establecen para su respectivo control.

#### 5.4. BUENAS PRÁCTICAS QUE PERMITAN GESTIONAR EL RIESGO BASADO EN ESTÁNDARES CON EL FIN GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN EN ESTAS ENTIDADES.

Los eventos anteriores indican la necesidad de reconocer la importancia de atender los procedimientos a nivel de seguridad en las entidades estatales, ejemplo de ellos son los registros presentados por el informe presentado en el año 2022 de la Cámara Colombiana de Informática y Telecomunicaciones CCIT, donde se referencia .

Figura 13. Informe de CCIT

| No. | Dominio.gov.co comprometido        | Credenciales expuestas | No.  | Dominio.gov.co comprometido       | Credenciales expuestas |
|-----|------------------------------------|------------------------|------|-----------------------------------|------------------------|
| 66  | muisca.dian.gov.co                 | 3,318                  | 703  | www.colpensiones.gov.co:8070      | 359                    |
| 226 | simo.cnsc.gov.co                   | 1,122                  | 744  | jovenesenaccion.dps.gov.co        | 339                    |
| 277 | www2.icfesinteractivo.gov.co       | 933                    | 813  | www.positivaenlinea.gov.co        | 307                    |
| 328 | personas.serviciodeempleo.gov.co   | 766                    | 837  | web.sispro.gov.co                 | 296                    |
| 446 | www.icetex.gov.co                  | 555                    | 893  | visibles.migracioncolombia.gov.co | 273                    |
| 461 | evaluarparaavanzar311.icfes.gov.co | 539                    | 910  | www.fna.gov.co:8081               | 265                    |
| 500 | sede.colpensiones.gov.co           | 499                    | 937  | snrbotondopago.gov.co             | 254                    |
| 512 | oficinavirtual.shd.gov.co          | 489                    | 943  | webazure.dian.gov.co              | 252                    |
| 573 | community.secop.gov.co             | 434                    | 1077 | solicitudes.icetex.gov.co         | 213                    |
| 605 | servidorpublico.sigep.gov.co       | 414                    | 1200 | www.medellin.gov.co               | 192                    |
| 629 | miseguridadsocial.gov.co           | 404                    | 1244 | ecenso.dane.gov.co                | 182                    |
| 682 | epagos.registraduria.gov.co        | 373                    | 1297 | www.funcionpublica.gov.co         | 176                    |

Fuente: Informe de CCIT: (2022): Disponible en : <https://www.ccit.org.co/wp-content/uploads/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno-safe-bp.pdf>

Por lo anterior, se observa un escenario donde las vulnerabilidades en las sedes electrónicas del estado colombiano se encuentran en constante ataque, por lo cual es relevante reconoce que se pueden establecer procedimientos de

buenas prácticas en el desarrollo de las actividades gestión de TI de las instituciones, ejemplo de ello es del reconocimiento de las acciones donde La información hace parte de uno de los activos más importantes en el amplio espectro de las diferentes organizaciones, ya sean del orden privado o público, comprendiendo y entendiéndose como elementos de que se deben salvaguardar con el ánimo de garantizar la Integralidad, Confidencialidad y Disponibilidad de la Información; es importante establecer procesos de jerarquización que permitan servir como guía en el desarrollo de los protocolos de que se deben adelantar los procesos de monitoreo, revisión y mejoramiento de los elementos de seguridad de la información, de tal forma que se pueda articular para fortalecer el Plan Estratégico de Tecnologías de Información – PETI , como un acción propia del desarrollo de los procesos institucionales, donde se pueda trazar un objetivo transversal basado en la identificación de los riesgos y aplicación de las acciones que permitan la minimización o materialización de los mismos.

Dentro de estos elementos se pueden reconocer procesos de control como los siguientes de acuerdo con los parámetros de integralidad confidencialidad y disponibilidad .

**Tabla 57. Parámetro de Integralidad, Confidencialidad y Disponibilidad.**

| <b>PARÁMETROS DE INTEGRALIDAD CONFIDENCIALIDAD Y DISPONIBILIDAD</b> |                                                                                                                                                                                                                       |                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>NIVEL</b>                                                        | <b>INTEGRALIDAD</b>                                                                                                                                                                                                   | <b>CONFIDENCIALIDAD</b>                                                                                                                                                                                                         | <b>DISPONIBILIDAD</b>                                                                                                                                                                                                                                                |
| <b>MÍNIMO</b>                                                       | La no disponibilidad de la información puede causar una leve afectación en las actividades cotidianas, y no tiene implicaciones legales y/o económicas.                                                               | Donde la Información se genere pérdida o alteración de esta puede causar un impacto poco significativo para el ente territorial.                                                                                                | La información que se clasifica como de conocimiento público, y la divulgación de esta no genera ninguna afectación negativa para el ente territorial.                                                                                                               |
| <b>BAJO</b>                                                         | La no disponibilidad de la información puede causar una afectación en las actividades cotidianas, y no tiene implicaciones legales y/o económicas.                                                                    | La Información, la cual por pérdida o alteración de esta genera un posible impacto negativo para el ente territorial.                                                                                                           | La información que se clasifica como de conocimiento público con ciertas restricciones, Y la divulgación de esta no genera ninguna afectación negativa a tercero o para el ente territorial.                                                                         |
| <b>MEDIO</b>                                                        | La no disponibilidad de la información puede causar una afectación en las actividades cotidianas, asimismo puede ser causal de implicaciones legales y/o económicas.                                                  | Se trata de la información donde la pérdida o alteración de esta, genera un posible impacto negativo para el ente territorial, lo cual puede generar situaciones de índole legal y/o económica.                                 | La información que se caracteriza como clasificada y es de uso de los funcionarios públicos y de terceros haciendo parte de los procesos internos Institucionales. Y la divulgación no autorizada puede impactar negativamente las actividades del ente territorial. |
| <b>ALTO</b>                                                         | La no disponibilidad de la información causa una afectación importante en las actividades cotidianas, asimismo puede ser causal de implicaciones legales y/o económicas.                                              | La Información donde la pérdida o alteración de esta genera un importante impacto negativo para el ente territorial, lo cual puede generar situaciones de índole legal y/o económica.                                           | La información que se clasifica como reservada. Y la divulgación no autorizada impacta negativamente las actividades del ente territorial.                                                                                                                           |
| <b>CRÍTICO</b>                                                      | La no disponibilidad de la información causa una afectación importante en las actividades cotidianas, asimismo puede ser causal de implicaciones legales y/o económicas y afectar gravemente la imagen institucional. | La Información donde la pérdida o alteración de esta genera un importante impacto negativo para ente territorial, lo cual puede generar situaciones de índole legal y/o económica y afectar gravemente la imagen institucional. | La información que se clasifica como reservada y es de uso exclusivo del usuario legítimo, cuenta con características y privilegios de usuario. Y la divulgación de esta impacta negativamente las actividades del ente territorial.                                 |

Fuente: Elaboración propia.

#### **5.4.1. Recomendaciones generales sobre activos de información:**

Los activos de información hacen parte fundamental de los datos que conforman las actividades cotidianas de los funcionarios en el desarrollo propio del ejercicio laboral. Dentro de los activos se determinan las características de este (tipo de dato, relevancia, ruta de almacenamiento, alojamiento, encriptación (si aplica), disponibilidad, duplicidad y accesos compartidos. En el ejercicio de valoración del activo se tienen presente (confidencialidad, integralidad y disponibilidad).

**5.4.1.1. Revisión.** La revisión de los activos se realiza de manera periódica, en tiempo de frecuencia temporal no mayores a 30 días, donde se genere un reporte de los procesos de seguridad de la información. Validando de esta forma el estado del activo.

**5.4.1.2. Gestión de control.** Los recursos digitales y medios de acceso serán validados por medio de contraseña segura en tanto para recursos web como para los locales y restricción de acceso a la red; solo generado rutas compartidas entre los equipos de trabajo directos, minimizando de esta forma el acceso y modificación de los datos, proporcionando un adecuado entorno de habilitación de los recursos compartidos en la red local. En el caso de los recursos compartidos en nube, se establecerán jerarquía en el ejercicio de acceso compartido, es decir cada líder de dependencia tendrá habilitado un fichero en la nube donde sincroniza la información de sus equipos de trabajo protegido por contraseña, de acuerdo de la necesidad del activo, manteniendo así la integralidad, confidencialidad y disponibilidad de la información, manteniendo un protocolo de contraseña segura .

### 5.4.2. Fichas de control para activos esenciales

Tabla 58. Formato para activos esenciales

| <i>[info] Información</i>                                                 |                |
|---------------------------------------------------------------------------|----------------|
| <b>código:</b>                                                            | <b>nombre:</b> |
| <b>descripción:</b>                                                       |                |
|                                                                           |                |
| <b>propietario:</b>                                                       |                |
| <b>responsable:</b>                                                       |                |
|                                                                           |                |
|                                                                           |                |
| <b>tipo</b> (marque todos los adjetivos que procedan)<br>Ver Sección 2.1. |                |
|                                                                           |                |

Fuente: Metodología magerit

Valoración de la información, típicamente en las siguientes dimensiones de seguridad:

[I] integridad

[C] confidencialidad

[A] autenticidad de los datos

[T] trazabilidad de los datos, quién ha modificado qué

**Tabla 59. Formato de valorización**

| <i>Valoración</i> |              |                      |
|-------------------|--------------|----------------------|
| <i>dimensión</i>  | <i>valor</i> | <i>justificación</i> |
| <i>[I]</i>        |              |                      |
| <i>[C]</i>        |              |                      |
| <i>[A]</i>        |              |                      |
| <i>[T]</i>        |              |                      |

Fuente: Metodología magerit

**Tabla 60. Formato de activos inferiores**

| <i>Dependencias de activos inferiores (hijos)</i> |        |
|---------------------------------------------------|--------|
| activo:                                           | grado: |
| ¿por qué?:                                        |        |
|                                                   |        |
| activo:                                           | grado: |
| ¿por qué?:                                        |        |
|                                                   |        |
| activo:                                           | grado: |
| ¿por qué?:                                        |        |
|                                                   |        |

Fuente: Metodología magerit

### **5.4.3. Descripción del mapa de riesgos**

1. Identificación del proyecto.
  - a. Código, descripción, propietario, organización.
  - b. Versión, fecha.
  - c. Biblioteca de referencia.

2. Activos
  - a. Árbol de activos (relaciones de dependencia)
  - b. Valoración de los activos (valor propio) Indicando la razón de la valoración atribuida a cada activo en cada dimensión.
3. Amenazas por activo Para cada activo:
  - a. amenazas relevantes
  - b. degradación estimada en cada dimensión
  - c. frecuencia anual estimada
4. Activos por amenaza Para cada amenaza:
  - a. activos afectados
  - b. degradación estimada en cada dimensión
  - c. frecuencia anual estimada

Por lo anterior. Se describen en su totalidad las acciones que comprenden el análisis de las brechas de seguridad en infraestructura de TI en las entidades territoriales de sexta categoría (Alcaldía) en el territorio colombiano mediante consulta de fuentes especializadas con el fin de proponer recomendaciones y buenas prácticas que permitan gestionar el riesgo. Proporcionando un recorrido por la identificación de brechas de seguridad en las entidades mencionadas, reconocimiento de los antecedentes en cuanto a los eventos registrados, descripción general del modelo de análisis de riesgo, y la presentación de buenas prácticas que permitan la gestión del riesgo.

## 6. CONCLUSIONES

El ministerio TIC, así como los respectivos informes de los CSIRT Colombia aportan información relevante sobre los procesos actuales de seguridad digital, en la nación, estos informes develan una realidad con respecto los riesgos de vulnerabilidad en los cuales se encuentra las entidades estatales, estos informes permitieron reconocer una realidad nacional y poder reconocer un contexto en la forma como se puede proceder para realización acciones de control en las entidades estatales.

Los eventos relacionados con la construcción de los procesos, evidencian las acciones que corresponden a los riesgos de seguridad digital en las entidades por lo cual, en el presente estudio se abordaron elementos concernientes a los elementos de riesgos que corresponden a los entes territoriales específicamente Alcaldías, donde las condiciones particulares de sexta categoría limita las acciones presupuestales para invertir en robustos sistemas de información, por lo cual es importantes explorar acciones que permitan aportar a la gestión de TI en las instituciones de manera más costo eficiente.

Un modelo de gestión de riesgo de TI es una herramienta esencial para las organizaciones que desean proteger sus sistemas y datos informáticos. Este modelo permitió a las organizaciones identificar, evaluar y mitigar los riesgos que pueden afectar su infraestructura TI, por lo cual dicha implementación aporta significativamente en la mejora de la seguridad de los sistemas de informáticos, minimiza el riesgo en cuanto a los datos e información financiera y mejora los procesos y procedimientos institucionales. Para implementar un modelo de gestión de riesgo de TI de manera exitosa, se recomienda contar con el apoyo de la alta gerencia, involucrar a todas las partes interesadas, establecer una cultura de seguridad, implementar controles efectivos y realizar auditorías periódicas. En este orden la importancia de un modelo de gestión de riesgo de TI radica en que permite a las organizaciones proteger sus sistemas y datos informáticos, lo que es esencial para su funcionamiento y éxito.

El apoyo de la alta gerencia es esencial para el éxito de cualquier iniciativa de gestión del riesgo. La alta gerencia debe estar comprometida con la seguridad de la

información y debe proporcionar los recursos necesarios para implementar las recomendaciones del modelo. Las entidades de sexta categoría suelen tener recursos limitados, por lo que es importante que adopten un enfoque proactivo y eficiente para la gestión del riesgo. A continuación, se presentan algunas recomendaciones específicas para estas entidades :

- **Enfoque basado en riesgos:** Las entidades de sexta categoría deben centrarse en los riesgos que tienen un impacto significativo en sus operaciones.
- **Implementación gradual:** Las entidades de sexta categoría pueden implementar un programa de gestión de riesgo de manera gradual, comenzando con los riesgos más críticos.
- **Utilización de herramientas y recursos disponibles:** Existen herramientas y recursos disponibles que pueden ayudar a las entidades de sexta categoría a implementar un programa de gestión de riesgo.

## **7. RECOMENDACIONES**

### **7.1. RECOMENDACIONES GENERALES**

Las recomendaciones generales que corresponden a las medidas de seguridad digital que se deben contemplar en las entidades de territoriales de sexta categoría específicamente Alcaldías se puede indicar lo siguiente:

#### **7.1.1. Contar con el apoyo de la alta gerencia**

El apoyo de la alta gerencia es esencial para el éxito de cualquier iniciativa de seguridad digital. La alta gerencia debe estar comprometida con la seguridad de la información y debe proporcionar los recursos necesarios para implementar las recomendaciones. Ya que de esta forma se pueden fortalecer las directrices de control, frente las acciones planes y políticas propias del control digital de la institución.

#### **7.1.2. Involucrar a todas las partes interesadas**

Es importante involucrar a todas las partes interesadas en el proceso de seguridad digital. Esto incluye a los empleados, los proveedores y los clientes. La participación de todas las partes interesadas ayudará a garantizar que las medidas sean efectivas y que se tengan en cuenta todos los riesgos. Siendo importante el desarrollo procesos de cultura digital, permitiendo fortalecer el conocimiento sobre la vulnerabilidad en las instituciones públicas, siendo el personal una de las brechas más comunes, de acuerdo a la recepción de correos electrónicos maliciosos.

#### **7.1.3. Establecer una cultura de seguridad**

La seguridad digital debe ser una prioridad para toda la organización. Es importante establecer una cultura de seguridad que promueva la concienciación y la responsabilidad en materia de seguridad. Esto se logra por medio de la implementación de capacitaciones de concientización para promover el desarrollo de los procesos digitales fundamentales en el ejercicio cotidiano de los funcionarios, es decir, reconocer elementos de riesgos como correos maliciosos, con remitentes no oficiales, con archivos comprimidos tipo .zip .rar o elementos tipo .SVG , los cuales son más comunes para transportar elementos de explotación

#### **7.1.4. Implementar controles efectivos**

Los controles son medidas que se implementan para mitigar los riesgos. Es importante implementar controles efectivos que sean adecuados para los riesgos identificados.

#### **7.1.5. Realizar auditorías periódicas**

Las auditorías periódicas son esenciales para evaluar la eficacia de las medidas de seguridad. Las auditorías deben realizarse por un equipo independiente que pueda proporcionar una evaluación objetiva.

### **7.2. RECOMENDACIONES ESPECIFICAS**

Las recomendaciones específicas que corresponden a las medidas de seguridad digital que se deben contemplar en las entidades de territoriales de sexta categoría específicamente Alcaldías se puede indicar lo siguiente:

#### **7.2.1. Adaptar las medidas a las características específicas de la alcaldía**

Las medidas de seguridad deben ser adaptadas a las características específicas de la alcaldía. Esto incluye su tamaño, sector y entorno operativo.

Dentro de estos procesos de control se debe fortalecer la cultura de seguridad digital, socializar con las áreas el riesgo más representativo, los controles frente a estas identificaciones. Establecer planes y políticas de tratamiento de riesgos y protección de la información, estos elementos deben estar inmersos de las acciones de las políticas gobierno digital y el Plan Estratégico de Tecnologías de las Información PETI.

Las alcaldías están expuestas a una serie de riesgos específicos, como ataques cibernéticos, fraudes y desastres naturales. Es importante considerar estos riesgos al implementar las medidas de seguridad. Dentro de estos procesos se deben considerar elementos de respaldo automatizado, copias de seguridad y protección de información ya sea en nube o servicios on premise. Asimismo, la formación Continua: La concienciación y capacitación en ciberseguridad debe ser constante. Los empleados son el primer punto de defensa.

Evaluación Continua: La realización de evaluaciones periódicas de riesgos y auditorías internas para asegurar que los controles de seguridad y las políticas de TI estén vigentes y efectivos.

Implementar un Sistema de Gestión de Incidentes: Definir claramente los procedimientos para identificar, responder y aprender de los incidentes de seguridad.

Alineación Estratégica de TI: Asegurar que la tecnología y las prácticas de seguridad soporten las metas y los objetivos generales del negocio.

## BIBLIOGRAFÍA

CAMILA, TRUJILLO. Casos de estudio de cybercrimen para el mejoramiento de la seguridad informática en pymes y medianas empresas - 10596/30220. Universidad Nacional Abierta y a Distancia UNAD - [página web]. (13, noviembre, 2019). [Consultado el 30, marzo, 2023]. Disponible en Internet: <http://repository.unad.edu.co/handle/10596/30220>

CANO . La seguridad de la información en la gestión de proyectos de TI: ¿Un análisis de vulnerabilidades es suficiente? ElNotariado.com [página web]. (2016) [Consultado el 30, marzo, 2023]. Disponible en: <http://www.elnotariado.com/la-seguridad-informacion-gestion-proyectos-ti-un-analisis-vulnerabilidades-suficiente-5963.html>

CERVANTES, ALEJANDRO. Seguridad lógica usando entornos de desarrollo en aplicaciones web empresariales. - 10596/33794. Universidad Nacional Abierta y a Distancia UNAD - [página web]. (16, mayo, 2020). [Consultado el 30, marzo, 2023]. Disponible en Internet: <http://repository.unad.edu.co/handle/10596/33794>

CHOQUE. Análisis Comparativo De Los Algoritmos Criptográficos Utilizados En Seguridad Informática [página web]. (2022). [Consultado el 30, marzo, 2023]. Disponible en: <http://ddigital.umss.edu.bo:8080/jspui/handle/123456789/29475>

CISCO. ¿Qué es la seguridad de red? Cisco [página web]. (15, febrero, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: [https://www.cisco.com/c/es\\_mx/products/security/what-is-network-security.html#~tipos](https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html#~tipos)

COLOMBIA AGIL. Categoría de los entes territoriales. Colombia Agil [página web]. (21, julio, 2020). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://www.colombiaagil.gov.co/tramites/intervenciones/categorizacion-municipios>

DEFINICIÓN. Definición de red de datos - Definicion.de. Definición.de [página web]. (13, febrero, 2019). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://definicion.de/red-de-datos/>

DELGADO SANTANA. Seguridad informática: Competencia digital docente en la gestión pedagógica de aula [página web]. (2022). [Consultado el 30, marzo, 2023]. Disponible en : . <http://repositorio.sangregorio.edu.ec:8080/handle/123456789/2738>

ESCOBAR BETANCUR. Análisis de vulnerabilidades y potenciales falencias de la empresa Servicios TI frente al Ransomwar [página web]. (2019). [Consultado el 30, marzo, 2023]. Disponible en: <https://repository.uniminuto.edu/handle/10656/11150>

FERNÁNDEZ. Pedro, Como implementar un SGSI. Como implementar un SGSI [página web]. (15, enero, 2018). Consultado el 01, abril, 2023]. Disponible en Internet: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624?page=14>

FERNÁNDEZ. Reveladas siete nuevas variantes de los ataques Meltdown y Spectre [página web]. (2018). [Consultado el 30, marzo, 2023.] Disponible en: <https://instituciones.sld.cu/dnspminsap/2018/11/16/reveladas-siete-nuevas-variantes-de-los-ataques-meltdown-y-spectre/>

FUNCIÓN PÚBLICA. Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones—Gestor Normativo—Función Pública [página web]. (2015). [Consultado el 30, marzo, 2023]. Disponible en Internet: . <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888>

HOLM [página web]. (2020). [Consultado el 30, marzo, 2023]. Transformación digital en el sector público de Estonia: Beneficios y desafíos para la Oficina Nacional de Auditoría. Revista española de control externo, 22(64), 22-47

HUAMANTINGO NAVARRO. Modelo para el análisis de vulnerabilidades digitales en una entidad pública de Lima, 2021. Repositorio Institucional - UCV. [página web]. (2022). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://repositorio.ucv.edu.pe/handle/20.500.12692/85150>

IMB. ¿Qué es infraestructura de TI? IBM - Deutschland | IBM [página web]. (20, abril, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://www.ibm.com/co-es/topics/infrastructure>

INTERNATIONAL. Historia de la Ciberseguridad. Plataforma Digital de Economía, Derecho y otras Ciencias Sociales y Humanas [página web]. (5, agosto, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://leyderecho.org/historia-de-la-ciberseguridad/>

ISO 27000 y el conjunto de estándares de Seguridad de la Información [Anónimo]. GlobalSuite Solutions [página web]. (15, marzo, 2018). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/>

JIMÉNEZ GARCÍA, SALAZAR BARRERA. Análisis de riesgos, amenazas y vulnerabilidades de la compañía Pinzon Pinzón & Asociados en su área de TI y planteamiento de los controles a aplicar basados en la norma ISO 27001: 2013. instname:Universidad Piloto de Colombia. [página web]. (2016). [Consultado el 30, marzo, 2023]. Disponible en Internet: <http://repository.unipiloto.edu.co/handle/20.500.12277/2727>

LOZANO, J. L. W.-B., & DAZA, E. F. [página web]. (2020). [Consultado el 30, marzo, 2023]. Blockchain: Instrumento de transparencia y control del sector público. Revista española de control externo, 22(64), 132-149.

MEN. ENTIDAD TERRITORIAL: - ...:Ministerio de Educación Nacional de Colombia:... MEN - Inicio [página web]. (10, mayo, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://www.mineducacion.gov.co/1621/article-82749.html#:~:text=Z-.ENTIDAD%20TERRITORIAL:,la%20Constitución%20y%20la%20ley.>

MINTIC. [página web]. (2020). [Consultado el 30, marzo, 2023]. PETI - Arquitectura TI. <https://www.mintic.gov.co/arquitecturati/630/w3-article-9148.html>

MINTIC. [página web]. (2016). [Consultado el 30, marzo, 2023]. Conpes | MINCIT - Ministerio de Comercio, Industria y Turismo. <https://www.mincit.gov.co/ministerio/normograma-sig/procesos-estrategicos/gestion-de-informacion-y-comunicacion/conpes>

MINTIC. Gobierno nacional publica borrador del decreto de ciberseguridad para el paÃ-s - Gobierno nacional publica borrador del decreto de ciberseguridad para el paÃ-s. MINTIC Colombia [página web]. (2022). [Consultado el 17, abril, 2023]. Disponible en Internet: <https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/198588:Gobierno-nacional-publica-borrador-del-decreto-de-ciberseguridad-para-el-pais.>

MORÁN MALDONADO, N. M. [página web]. (2021). [Consultado el 30, marzo, 2023]. Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática [BachelorThesis]. <http://dspace.ups.edu.ec/handle/123456789/20243>

MUÑOZ, P., & CAMILO, C. [página web]. (2019). [Consultado el 30, marzo, 2023]. Análisis de metodologías de Ethical hacking para la detección de vulnerabilidades en las Pymes. <http://repository.unad.edu.co/handle/10596/30302>

MUÑOZ, ZAPATA, REQUENA, & RICARDO. [página web]. (2019). [Consultado el 30, marzo, 2023]. Riesgos informáticos y alternativas para la seguridad informática

en sistemas contables en Colombia. Revista Venezolana de Gerencia. <https://doi.org/10.37960/revista.v24i2.31508>

NACIONAL, Á. DE N. Y S. DE C. DEL C. C. [página web]. (2020). [Consultado el 30, marzo, 2023]. La ciberseguridad y su relevancia en el Sector Público: El papel del Centro Criptológico Nacional. Revista española de control externo, 22(64), 66-87.

ODAR GUERRERO, A. Y. S. [página web]. (2018). [Consultado el 30, marzo, 2023]. Propuesta de una auditoria de seguridad para el manejo de vulnerabilidades de la red informática de la Universidad Señor de Sipán. Universidad de Lambayeque. <https://repositorio.udl.edu.pe/jspui/handle/UDL/194>

PARRA CALDERÓN, J. A. [página web]. (2019). [Consultado el 30, marzo, 2023]. Delitos informáticos y marco normativo en Colombia. <http://repository.unad.edu.co/handle/10596/28115>

RÍO FERNÁNDEZ. Gabriel, [página web]. (2022). [Consultado el 30, marzo, 2023]. Integración de una solución software ITSM con bases de datos de vulnerabilidades para la mejora de la ciberseguridad de las infraestructuras y sistemas TI. <https://digibuo.uniovi.es/dspace/handle/10651/64444>

RODRÍGUEZ [página web]. (2021). [Consultado el 30, marzo, 2023]. Buenas prácticas de seguridad informática aplicado al comercio electrónico para las Pymes colombianas asociada a la norma ISO 27001:2013 Anexo A. <http://repository.unad.edu.co/handle/10596/42688>

SÁNCHEZ GAMBOA. Luis, [página web]. (2019). [Consultado el 30, marzo, 2023]. Identificación de vulnerabilidades y riesgos en los activos de ti de energitel. <http://repository.unad.edu.co/handle/10596/28221>

SOTO, Leyre. ¿Qué es la seguridad digital? Welcome to the Signaturit blog [página web]. (15, abril, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://blog.signaturit.com/es/que-es-seguridad-digital>

TECNOLOGÍA INFORMATICA. Sistema de Información. Tecnologia Informatica [página web]. (30, mayo, 2019). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://www.tecnologia-informatica.com/que-es-sistema-informacion/>

ZAMBRANO LOOR. [página web]. (2021). [Consultado el 30, marzo, 2023]. Diseño de modelo de seguridad y plan de mejoras para la seguridad de la red, en función de las vulnerabilidades y amenazas detectadas en la empresa CENFORSP. CIA LTDA. Disponible: <https://repositorio.ecotec.edu.ec/handle/123456789/273>

## 8. ANEXO

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fecha de Realización:</b> 10/12/2024                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Título:</b> ANÁLISIS SOBRE LAS VULNERABILIDADES EN LA INFRAESTRUCTURA DE TI DE LAS ENTIDADES TERRITORIALES DE SEXTA CATEGORÍA (ALCALDÍAS) EN TERRITORIO COLOMBIANO.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Autor:</b> Holguin Carvajal, Luis Alberto                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Palabras Claves:</b> Infraestructura de TI, normatividad, redes de datos, seguridad digital, tecnologías de la información                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Descripción:</b> La seguridad digital hace parte fundamental de los procesos de control que se deben adoptar en las instituciones, por tanto Identificar las vulnerabilidades se convierte en una de las acciones que se deben priorizar en los entornos de protección de las infraestructuras de TI, pero en algunos casos de estos procesos de implementación tienden a ser costos, y el conocimiento aplicado desde una espectro ingenieril, representan limitaciones para el desarrollo objetivos de tan importantes procesos para el desarrollo fundamentado en la protección de las información, siendo consecuente con la necesidad de aplicar elementos de control y gestión como: almacenamiento en la nube, CRM, Firewall, sistemas robusto de protección de información, respaldos automatizados entre otros, por lo cual los procesos de detención temprana son vitales para este tipo de infraestructura, donde la capacidad financiera requiere de una mejor gestión acorde con la capacidad instalada, proporcionando así dinámicas que aporten al mejoramiento escalado de dicha capacidad, siendo importante la necesidad de reconocer e implementar elementos de gestión de riesgos, analizando brechas de seguridad de TI, con la finalidad de permitir generar recomendaciones y buenas prácticas en el sector. Es por ello, que el objetivo principal de este proyecto es Analizar las brechas de seguridad en infraestructura de TI en las entidades territoriales de sexta categoría (Alcaldía) en el territorio colombiano mediante consulta de fuentes especializadas con el fin de proponer recomendaciones y buenas prácticas que permitan gestionar el riesgo. Este análisis busca la identificación de mecanismos que aporten de manera significativa a minimizar riesgos, ya que si no se logra establecer estos procesos la infraestructura de información, generará vulnerabilidades que pueden afectar la misionalidad de la institución, por lo cual, estos riesgos deben abordarse desde las condiciones técnicas de infraestructura de TI, de manera transversal donde se tenga presente los aspectos sociales y de comportamiento, donde se relaciona al ser humano dentro del factor de vulnerabilidad, siendo una de las falencias visibles al momento de un atacante utilizar vectores como correos electrónicos como medio |

de infiltración, por lo tanto, es importante generar estrategias que permitan de manera objetiva al control de los riesgos, o en el mejor de los casos evitando la materialización de los mismos .

**Fuentes:**

- CAMILA, TRUJILLO. Casos de estudio de cybercrimen para el mejoramiento de la seguridad informática en pymes y medianas empresas - 10596/30220. Universidad Nacional Abierta y a Distancia UNAD - [página web]. (13, noviembre, 2019). [Consultado el 30, marzo, 2023]. Disponible en Internet: <http://repository.unad.edu.co/handle/10596/30220>
- CANO . La seguridad de la información en la gestión de proyectos de TI: ¿Un análisis de vulnerabilidades es suficiente? ElNotariado.com [página web]. (2016) [Consultado el 30, marzo, 2023]. Disponible en: <http://www.elnotariado.com/la-seguridad-informacion-gestion-proyectos-ti-un-analisis-vulnerabilidades-suficiente-5963.html>
- CERVANTES, ALEJANDRO. Seguridad lógica usando entornos de desarrollo en aplicaciones web empresariales. - 10596/33794. Universidad Nacional Abierta y a Distancia UNAD - [página web]. (16, mayo, 2020). [Consultado el 30, marzo, 2023]. Disponible en Internet: <http://repository.unad.edu.co/handle/10596/33794>
- CHOQUE. Análisis Comparativo De Los Algoritmos Criptográficos Utilizados En Seguridad Informática [página web]. (2022). [Consultado el 30, marzo, 2023]. Disponible en: <http://ddigital.umss.edu.bo:8080/jspui/handle/123456789/29475>
- CISCO. ¿Qué es la seguridad de red? Cisco [página web]. (15, febrero, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: [https://www.cisco.com/c/es\\_mx/products/security/what-is-network-security.html#~tipos](https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html#~tipos)
- COLOMBIA AGIL. Categoría de los entes territoriales. Colombia Agil [página web]. (21, julio, 2020). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://www.colombiaagil.gov.co/tramites/intervenciones/categorizacion-municipios>
- DEFINICIÓN. Definición de red de datos - Definicion.de. Definición.de [página web]. (13, febrero, 2019). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://definicion.de/red-de-datos/>
- DELGADO SANTANA. Seguridad informática: Competencia digital docente en la gestión pedagógica de aula [página web]. (2022).

[Consultado el 30, marzo, 2023]. Disponible en : .  
<http://repositorio.sangregorio.edu.ec:8080/handle/123456789/2738>

- ESCOBAR BETANCUR. Análisis de vulnerabilidades y potenciales falencias de la empresa Servicios TI frente al Ransomware [página web]. (2019). [Consultado el 30, marzo, 2023]. Disponible en: <https://repository.uniminuto.edu/handle/10656/11150>
- FERNÁNDEZ. Pedro, Como implementar un SGSI. Como implementar un SGSI [página web]. (15, enero, 2018). Consultado el 01, abril, 2023]. Disponible en Internet: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624?page=14>
- FERNÁNDEZ. Reveladas siete nuevas variantes de los ataques Meltdown y Spectre [página web]. (2018). [Consultado el 30, marzo, 2023.] Disponible en: <https://instituciones.sld.cu/dnspminsap/2018/11/16/reveladas-siete-nuevas-variantes-de-los-ataques-meltdown-y-spectre/>
- FUNCIÓN PÚBLICA. Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones—Gestor Normativo—Función Pública [página web]. (2015). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888>
- HOLM [página web]. (2020). [Consultado el 30, marzo, 2023]. Transformación digital en el sector público de Estonia: Beneficios y desafíos para la Oficina Nacional de Auditoría. Revista española de control externo, 22(64), 22-47
- HUAMANTINGO NAVARRO. Modelo para el análisis de vulnerabilidades digitales en una entidad pública de Lima, 2021. Repositorio Institucional - UCV. [página web]. (2022). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://repositorio.ucv.edu.pe/handle/20.500.12692/85150>
- IMB. ¿Qué es infraestructura de TI? IBM - Deutschland | IBM [página web]. (20, abril, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://www.ibm.com/co-es/topics/infrastructure>
- INTERNATIONAL. Historia de la Ciberseguridad. Plataforma Digital de Economía, Derecho y otras Ciencias Sociales y Humanas [página web]. (5, agosto, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://leyderecho.org/historia-de-la-ciberseguridad/>
- ISO 27000 y el conjunto de estándares de Seguridad de la Información [Anónimo]. GlobalSuite Solutions [página web]. (15, marzo, 2018).

[Consultado el 30, marzo, 2023]. Disponible en Internet: <https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/>

- JIMÉNEZ GARCÍA, SALAZAR BARRERA. Análisis de riesgos, amenazas y vulnerabilidades de la compañía Pinzon Pinzón & Asociados en su área de TI y planteamiento de los controles a aplicar basados en la norma ISO 27001: 2013. instname:Universidad Piloto de Colombia. [página web]. (2016). [Consultado el 30, marzo, 2023]. Disponible en Internet: <http://repository.unipiloto.edu.co/handle/20.500.12277/2727>
- LOZANO, J. L. W.-B., & DAZA, E. F. [página web]. (2020). [Consultado el 30, marzo, 2023]. Blockchain: Instrumento de transparencia y control del sector público. Revista española de control externo, 22(64), 132-149.
- MEN. ENTIDAD TERRITORIAL: - ...:Ministerio de Educación Nacional de Colombia:... MEN - Inicio [página web]. (10, mayo, 2021). [Consultado el 30, marzo, 2023]. Disponible en Internet: <https://www.mineducacion.gov.co/1621/article-82749.html#:~:text=Z-ENTIDAD%20TERRITORIAL:,la%20Constitución%20y%20la%20ley.>
- MINTIC. [página web]. (2020). [Consultado el 30, marzo, 2023]. PETI - Arquitectura TI. <https://www.mintic.gov.co/arquitecturati/630/w3-article-9148.html>
- MINTIC. [página web]. (2016). [Consultado el 30, marzo, 2023]. Conpes | MINCIT - Ministerio de Comercio, Industria y Turismo. <https://www.mincit.gov.co/ministerio/normograma-sig/procesos-estrategicos/gestion-de-informacion-y-comunicacion/conpes>
- MINTIC. Gobierno nacional publica borrador del decreto de ciberseguridad para el país - Gobierno nacional publica borrador del decreto de ciberseguridad para el país. MINTIC Colombia [página web]. (2022). [Consultado el 17, abril, 2023]. Disponible en Internet: <https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/198588:Gobierno-nacional-publica-borrador-del-decreto-de-ciberseguridad-para-el-pais.>
- MORÁN MALDONADO, N. M. [página web]. (2021). [Consultado el 30, marzo, 2023]. Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática [BachelorThesis]. <http://dspace.ups.edu.ec/handle/123456789/20243>
- MUÑOZ, P., & CAMILO, C. [página web]. (2019). [Consultado el 30, marzo, 2023]. Análisis de metodologías de Ethical hacking para la detección de vulnerabilidades en las Pymes. <http://repository.unad.edu.co/handle/10596/30302>

**Contenido del documento:**

El contenido del documento consta de seis etapas en la primera se explica la problemática de la investigación, en la segunda y tercera parte los objetivos relacionados con el problema identificado, en la cuarta todo lo relacionado con el marco referencial, marco teórico, definiciones, marco conceptual, marco histórico, marco tecnológico, infraestructura TI, redes de datos, seguridad digital, ente territorial en la quinta fase desarrollo de los objetivos, brechas de seguridad de los entes territoriales, antecedentes de eventos de vulnerabilidad, modelo de gestión del riesgo basado en las características de infraestructura TI, buenas prácticas que permiten gestionar el riesgo basado en estándares con el fin de gestionar la seguridad de la información en estas entidades, sexta fase conclusiones y séptima fase recomendaciones.

**Metodología:**

El modelo se basa en los siguientes pasos:

- **Identificación de los activos de información críticos.** En este paso se identifican los activos de información que son esenciales para el funcionamiento de la alcaldía. Estos activos pueden ser datos, sistemas, aplicaciones, infraestructura, entre otros.
- **Evaluación de los riesgos.** En este paso se evalúan los riesgos que pueden afectar los activos de información identificados. Los riesgos pueden ser de origen natural, tecnológico, humano, entre otros.
- **Análisis de impacto.** En este paso se analiza el impacto que tendría la materialización de cada riesgo sobre los activos de información críticos.
- **Priorización de los riesgos** En este paso se priorizan los riesgos de acuerdo con su impacto.
- **Implementación de controles.** En este paso se implementan controles para mitigar los riesgos priorizados.

**Conceptos nuevos:**

- **VULNERABILIDAD:** Se trata de los factores que inciden en la identificación de los riesgos, donde el delincuente informático puede realizar intrusiones por medio de diferentes vectores de ataque.
- **RIESGO DIGITAL:** Elementos débiles dentro de una estructura digital, la cual puede ser interpretada como una vulnerabilidad

- **INCIDENCIA:** Es la ocurrencia de uno o varios eventos que puedan afectar la integridad, la confidencialidad y la disponibilidad de la información, como hechos que afectan las políticas de seguridad establecidas en una organización.
- **VECTOR DE ATAQUE:** Hace referencia al método utilizado por un delincuente informático para ingresar a un determinado sistema de información.
- **BACKUP:** Se trata de la información que puede ser respaldada, en proceso denominado copia de respaldo o copia de seguridad.
- **AUTENTICACIÓN:** Proceso con el cual un usuario se identifica en un sistema de información.
- **CERTIFICADO DIGITAL:** Hacer referencia a un documento informático generado por un prestador de servicios de certificación para garantizar la autenticidad del recurso digital al cual se está accediendo.
- **CIBERSEGURIDAD:** Es la actividad o práctica que busca proteger, los activos de información, equipos, redes de datos y software, que se pueden representar como sistemas críticos para la operación de las actividades de las organizaciones.
- **CRİPTOGRAFÍA:** Se trata de la protección de información por medio algoritmos que cuentan con diferentes estructuras de codificación para establecer procesos protección de datos, firmas digitales y demás elementos de privacidad o reserva.
- **FIREWALL:** Sistema de seguridad de red que permite controlar y/o restringir el tráfico de una red, con fines de protección de información.

**Conclusiones:** El ministerio TIC, así como los respectivos informes de los CSIRT Colombia aportan información relevante sobre los procesos actuales de seguridad digital, en la nación, estos informes develan una realidad con respecto los riesgos de vulnerabilidad en los cuales se encuentra las entidades estatales, estos informes permitieron reconocer una realidad nacional y poder reconocer un contexto en la forma como se puede proceder para realización acciones de control en las entidades estatales.

Los eventos relacionados con la construcción de los procesos, evidencian las acciones que corresponden a los riesgos de seguridad digital en las entidades por lo cual, en el presente estudio se abordaron elementos concernientes a los elementos de riesgos que corresponden a los entes territoriales específicamente Alcaldías, donde las condiciones particulares de sexta categoría limita las acciones presupuestales para invertir en robustos sistemas de información, por lo

cual es importantes explorar acciones que permitan aportar a la gestión de TI en las instituciones de manera más costo eficiente.

Un modelo de gestión de riesgo de TI es una herramienta esencial para las organizaciones que desean proteger sus sistemas y datos informáticos. Este modelo permitió a las organizaciones identificar, evaluar y mitigar los riesgos que pueden afectar su infraestructura TI, por lo cual dicha implementación aporta significativamente en la mejora de la seguridad de los sistemas de informáticos, minimiza el riesgo en cuanto a los datos e información financiera y mejora los procesos y procedimientos institucionales. Para implementar un modelo de gestión de riesgo de TI de manera exitosa, se recomienda contar con el apoyo de la alta gerencia, involucrar a todas las partes interesadas, establecer una cultura de seguridad, implementar controles efectivos y realizar auditorías periódicas. En este orden la importancia de un modelo de gestión de riesgo de TI radica en que permite a las organizaciones proteger sus sistemas y datos informáticos, lo que es esencial para su funcionamiento y éxito.

El apoyo de la alta gerencia es esencial para el éxito de cualquier iniciativa de gestión del riesgo. La alta gerencia debe estar comprometida con la seguridad de la información y debe proporcionar los recursos necesarios para implementar las recomendaciones del modelo. Las entidades de sexta categoría suelen tener recursos limitados, por lo que es importante que adopten un enfoque proactivo y eficiente para la gestión del riesgo. A continuación, se presentan algunas recomendaciones específicas para estas entidades :

- **Enfoque basado en riesgos:** Las entidades de sexta categoría deben centrarse en los riesgos que tienen un impacto significativo en sus operaciones.
- **Implementación gradual:** Las entidades de sexta categoría pueden implementar un programa de gestión de riesgo de manera gradual, comenzando con los riesgos más críticos.
- **Utilización de herramientas y recursos disponibles:** Existen herramientas y recursos disponibles que pueden ayudar a las entidades de sexta categoría a implementar un programa de gestión de riesgo.

**AUTOR:** Luis Alberto Holguin Carvajal