DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS MISIONALES DE LICENCIAMIENTO URBANÍSTICO Y OTRAS ACTUACIONES DE LA CURADURÍA URBANA No.3 ARQ. ANA MARÍA CADENA TOBÓN, CON BASE A LA NORMA ISO/IEC 27001:2013

JOHN FREDY CASTELLANOS
JEISSON JAVIER GOMEZ TORRES

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA, D.C.
2021

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS MISIONALES DE LICENCIAMIENTO URBANÍSTICO Y OTRAS ACTUACIONES DE LA CURADURÍA URBANA NO.3 ARQ. ANA MARÍA CADENA TOBÓN, CON BASE A LA NORMA ISO/IEC 27001:2013

JOHN FREDY CASTELLANOS
JEISSON JAVIER GÓMEZ TORRES

Trabajo de grado para optar el título de
Especialista en Seguridad Informática

Asesor
ÁLVARO ESCOBAR ESCOBAR
Director en Especialización en Seguridad Informática

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA, D.C.
2021

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____
Presidente del Jurado

_____
Jurado

_____
Jurado

Bogotá D.C., marzo de 2021

Dedicado a nuestras familias, quienes siempre creyeron en nosotros, siempre nos brindaron su apoyo de una manera incondicional, y siempre nos brindaron una voz de aliento en momentos críticos, familia es la muestra más fiel de apoyo comprensión y perseverancia.

AGRADECIMIENTOS

Agradecemos a Dios el permitirnos llegar a esta etapa profesional, a nuestros padres y a las personas que directa o indirectamente nos ofrecieron su apoyo para llevar este proyecto a la realidad, a la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, por depositar su confianza en nosotros como profesionales y a la Universidad Piloto de Colombia por formarnos y crear en nosotros profesionales con calidad de servicio y mente propositiva.

Ing. John Fredy Castellanos

Ing. Jeisson Javier Gómez Torres

CONTENIDO

	pág.
INTRODUCCIÓN	17
1. JUSTIFICACIÓN	19
2. PLANTEAMIENTO DEL PROBLEMA	21
2.1 FORMULACIÓN DEL PROBLEMA	21
3. OBJETIVOS	22
3.1 OBJETIVO GENERAL	22
3.2 OBJETIVOS ESPECÍFICOS	22
4. MARCO TEORICO	23
4.1 LA EMPRESA	23
4.1.1 Antecedentes del Curador Urbano.	23
4.1.2 El Curador Urbano.	23
4.1.3 La Curaduría Urbana.	23
4.1.4 Marco institucional.	24
4.1.4.1 Productos y servicios	24
4.1.4.2 Stakeholders.	24
4.1.4.3 Direccionamiento estratégico	25
4.1.4.4 Mapa de procesos	27
4.1.4.5 Estructura organizacional	27
4.1.5 Definición de los procesos de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.	28
4.1.6 Procesos misionales.	29
4.2 SEGURIDAD DE LA INFORMACIÓN	30
4.3 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	30
4.4 NORMA ISO/IEC 27001:2013	30
4.5 NORMA ISO 27002	31
4.6 NORMA ISO 27003	32
4.7 NTC-ISO 31000	32
4.8 CICLO PHVA	33
5. DISEÑO METODOLÓGICO	34
5.1 FASE DE EXPLORACIÓN	34
5.1.1 Subfase de acercamiento a la organización.	34
5.1.2 Subfase de diagnóstico	35
5.1.2.1 Resultados diagnóstico	35
5.2 FASE DE INTERVENCIÓN	54
5.2.1 Subfase de diseño de SGSI	54

6. IDENTIFICACIÓN DE ACTIVOS 57
6.1 ACTIVOS EN PROCESOS MISIONALES 57
6.2 VALORACIÓN DE ACTIVOS 62
6.2.1 Atributos de seguridad 62
6.2.2 Ponderado general de criterios 63

7. ANALISIS DEL RIESGO 68
7.1 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES 68

8. VALORACIÓN DEL RIESGO 70
8.1 MATRIZ VALORACIÓN DEL RIESGO 70
8.2 CRITERIOS APLICADOS PARA VALORACIÓN DE RIESGOS 71
8.2.1 Riesgo bajo valor 1-2 71
8.2.2 Riesgo medio valor 3-4 71
8.2.3 Riesgo alto valor 5-6 71
8.2.4 Riesgo critico 7-9 71
8.2.5 Aceptación de los riesgos 71
8.3 MAPA DE CALOR 77

9. TRATAMIENTO DE RIESGOS 79
9.1 SEGREGACIÓN DE CONTROLES 79
9.2 RESULTADO RESIDUAL 100

10. CREACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 101
10.1 ELEMENTOS DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 101
10.1.1 Objetivo. 101
10.1.1.1 Alcance 101
10.1.1.2 Generalidad 101
10.1.1.3 Desarrollo de directrices de seguridad de la información 101
10.1.1.4 Atributos de responsabilidades 104
10.1.1.5 Comité de gestión de seguridad 106
10.1.1.6 Propietarios de la información 106
10.2 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA CURADURIA N. 3 ARQ. ANA MARIA CADENA TOBÓN 107
10.2.1 Política seguridad de los recursos humanos 107
10.2.2 Política de gestión de activos 108
10.2.3 Política de control de acceso 109
10.2.4 Política de seguridad física y del entorno 111
10.2.5 Políticas de seguridad de la operación del negocio 113
10.2.6 Política de seguridad de las comunicaciones 114
10.2.7 Políticas de seguridad con proveedores 116

11. PLAN DE CONCIENCIACIÓN 117
11.1 GENERALIZACIÓN 117

11.1.1 Conciencia. 117
11.1.2 Entrenamiento. 117
11.1.3 Educación. 118
11.2 OBJETIVO 120
11.3 ALCANCE 120
11.4 ESTRATEGIA 120
11.4.1 Desarrollo en escenario 121
11.4.1.1 Socialización por medio de reuniones 121
11.4.1.2 Capacitaciones a usuarios con temáticas definidas. 121
11.4.1.3 Elaboración de campaña visual para los usuarios 124
11.4.1.4 Entrega de información útil de bolsillo 125
11.4.1.5 Envió de correos masivos socializando las políticas 129
11.4.1.6 Evaluaciones elaboradas por medio de formularios 129

12. CONCLUSIONES 131

BIBLIOGRAFÍA 134

ANEXOS 136

LISTA DE FIGURAS

pág.

Figura 1. Mapa de procesos Curaduría Urbana No.3 Arq. Ana María Cadena Tobón. 27
Figura 2. Procesos misionales Curaduría Urbana No. 3 29
Figura 3. Ciclo PHVA Grafica 33
Figura 4. Elementos del SGSI en la Curaduría Urbana No.3 56
Figura 5. Ponderado de los criterios para la valoración de los activos. 63
Figura 6. Conjunto de aprendizaje sobre seguridad TI. 118
Figura 7. Modelo de gestión de programa centralizada 119
Figura 8. Información Cartelera 124
Figura 9. Fondos de pantalla seguridad de la información 125
Figura 10. Catálogos sobre seguridad informática 1. 126
Figura 11. Catálogos sobre seguridad informática 2. 127
Figura 12. Catálogos sobre seguridad informática 3. 128
Figura 13. Correo masivo 129
Figura 14. Cuestionario ISO/IEC 27001:2013 funcionarios. 130

LISTA DE GRÁFICAS

pág.

Gráfica 1. Estado Inicial de la Curaduría Urbana No. 3 - General. 36
Gráfica 2. Estado inicial de la Curaduría Urbana No. 3 Políticas de la seguridad de la información 36
Gráfica 3. Estado actual de la Curaduría Urbana No. 3 37
Gráfica 4. Estado actual de la Curaduría Urbana No. 3 Seguridad de los recursos humanos 37
Gráfica 5. Estado actual de la Curaduría Urbana No. 3 Gestión de activos 38
Gráfica 6. Estado actual de la Curaduría Urbana No. 3 Control de acceso 38
Gráfica 7. Estado actual de la Curaduría Urbana No. 3 Criptografía. 39
Gráfica 8. Estado actual de la Curaduría Urbana No. 3 Seguridad física y del entorno 39
Gráfica 9. Estado actual de la Curaduría Urbana No. 3 Seguridad de las operaciones. 40
Gráfica 10. Estado actual de la Curaduría Urbana No. 3 Seguridad de las comunicaciones 40
Gráfica 11. Estado actual de la Curaduría Urbana No. 3 Adquisición, desarrollo y mantenimiento de sistemas 41
Gráfica 12. Estado actual de la Curaduría Urbana No. 3 Relaciones con los proveedores 41
Gráfica 13. Estado actual de la Curaduría Urbana No. 3 Gestión de incidentes de seguridad de la información 42
Gráfica 14. Estado actual de la Curaduría Urbana No. 3 Aspectos de seguridad de la información de la gestión de continuidad de negocio 42
Gráfica 15. Estado actual de la Curaduría Urbana No. 3 Cumplimiento 43
Gráfica 16. Test de Cumplimiento Norma ISO/IEC 27001:2013. La Organización y su Contexto. 44
Gráfica 17. Test de Cumplimiento Norma 27001:2013. La Organización y su Contexto 2. 44
Gráfica 18. Test de Cumplimiento Norma 27001:2013. La Organización y su Contexto 3 45
Gráfica 19. Test de Cumplimiento Norma 27001:2013. La Organización y su Contexto 4 45
Gráfica 20. Test de Cumplimiento Norma 27001:2013. La Organización y su contexto 5 46
Gráfica 21. Test de Cumplimiento Norma 27001:2013. Liderazgo 1 46
Gráfica 22. Test de Cumplimiento Norma 27001:2013. Liderazgo 2 47
Gráfica 23. Test de Cumplimiento Norma 27001:2013. Planificación 1 47
Gráfica 24. Test de Cumplimiento Norma 27001:2013. Planificación 2 48
Gráfica 25. Test de Cumplimiento Norma 27001:2013. Soporte 1 48
Gráfica 26. Test de Cumplimiento Norma 27001:2013. Soporte 2 49
Gráfica 27. Test de Cumplimiento Norma 27001:2013. Soporte 3 49

Gráfica 28. Test de Cumplimiento Norma 27001:2013. Soporte 4 50
Gráfica 29. Test de Cumplimiento Norma 27001:2013. Soporte 5 50
Gráfica 30. Test de Cumplimiento Norma 27001:2013. Operación 51
Gráfica 31. Test de Cumplimiento Norma 27001:2013. Evaluación del desempeño 1 52
Gráfica 32. Test de Cumplimiento Norma 27001:2013. Evaluación del desempeño 2 52
Gráfica 33. Test de Cumplimiento Norma 27001:2013. Mejora 53
Gráfica 34. Inventario general Curaduría Urbana 3. 57

LISTA DE CUADROS

pág.

Cuadro 1. Estadísticas boletín de seguridad Kaspersky 19
Cuadro 2. Estructura organizacional 28
Cuadro 3. Inventario Global Curaduría Urbana No. 3 - Parte 1 58
Cuadro 4. Inventario Global Curaduría Urbana No. 3 Parte 2 60
Cuadro 5. Niveles de los criterios para la valoración de los activos. 63
Cuadro 6. Cualificación valoración de activos. 64
Cuadro 7. Valoración de activos Curaduría Urbana No. 3. 65
Cuadro 8. Identificación de amenazas y vulnerabilidades 68
Cuadro 9. Probabilidades valoración del riesgo 70
Cuadro 10. Impacto valoración del riesgo 70
Cuadro 11. Probabilidad por impacto valoración del riesgo 71
Cuadro 12. Valoración de riesgo activo de información 72
Cuadro 13. Mapa de calor 78
Cuadro 14. Controles por amenaza 79
Cuadro 15. Tratamiento de riesgos 81
Cuadro 16. Cronograma de capacitaciones 122

LISTA DE ANEXOS

pág.

Anexo A. Acta de reunión 1 136
Anexo B. Acta de reunion 2 137
Anexo C. Acta de reunion 3 138
Anexo D. Procedimiento de radicacion 139
Anexo E. Procedimiento de radicación inicial 140
Anexo F. Procedimiento de radicación anexos 144
Anexo G. Diagnostico iso 27001 147

GLOSARIO

ACCIÓN CORRECTIVA: acción para eliminar la causa de una no conformidad y para prevenir la recurrencia. [1]

ACEPTACIÓN DEL RIESGO: informada decisión de tomar un riesgo en particular. La aceptación del riesgo puede ocurrir sin tratamiento del riesgo o durante el proceso de tratamiento del riesgo. Los riesgos aceptados están sujetos a supervisión y revisión.[2]

ACTIVO (ASSET): cualquier cosa que tenga valor para un individuo, una organización o un gobierno.[3]

ACTIVO DE LA INFORMACIÓN: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas de información, infraestructura de hardware y comunicaciones, edificios, personas, entre otros) que tenga valor para la organización.[4]

ALTA DIRECCIÓN: persona o grupo de personas que dirige y controla una organización al más alto nivel. La alta dirección (o alta gerencia) tiene el poder de delegar autoridad y proporcionar recursos dentro de la organización. [5]

AMENAZA: causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.[6]

ANÁLISIS DE RIESGO: proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo. El análisis de riesgo proporciona la base para la evaluación del riesgo y las decisiones sobre el tratamiento de riesgos.[7]

AUTENTICACIÓN: prestación de la garantía que una característica reclamada de una entidad es correcta.[8]

BASE DE DATOS: una base de datos es un conjunto estructurado de datos que representa entidades y sus interrelaciones. La representación será única e

---

[1] INTERNATIONAL STANDAR ORGANIZATION. ISO 27000. [en línea]. USA: La entidad [citado 3, junio, 2020]. Disponible en Internet: < URL: http://www.iso27000.es/glosario.html>
[2] Ibíd., p.2.
[3] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Glosario. [en línea]. Bogotá: El Ministerio [citado 8, enero, 2020]. Disponible en Internet: < URL: https://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7742.html>.
[4] Ibid., p.2.
[5] INTERNATIONAL STANDAR ORGANIZATION, Op. cit., p.2.
[6] Ibíd., p.2.
[7] Ibíd., p.2.
[8] Ibíd., p.1.

integrada, a pesar de que debe permitir utilizaciones varias y simultáneas. [9]

CONFIDENCIALIDAD: propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos.[10]

CONTROL: medida por la que se modifica el riesgo. Mecanismos como políticas, procedimientos y prácticas adoptados por las organizaciones para mantener los riesgos identificados por debajo del nivel del riesgo asumido.[11]

CONTROL DE ACCESO: significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad. [12]

DISPONIBILIDAD: propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada.[13]

FIREWALL: es un sistema diseñado para para prohibir o permitir el acceso desde o hacia una red. Un firewall puede ser físico o digital (virtual), es decir, puede estar en un dispositivo dedicado o trabajar cómo cortafuegos como un programa software, indispensable para mantener la seguridad de su red, especialmente a la hora de conectar a internet.[14]

GESTIÓN DE RIESGOS: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.[15]

IMPACTO: el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros. [16]

INCIDENTE DE SEGURIDAD DE INFORMACIÓN: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.[17]

INGENIERÍA SOCIAL: es un conjunto de técnicas que usan los cibercriminales para

---

[9] CAMPS, Rafael; CASILLAS, Luis; COSTAL, Dolors; GINESTÀ, Marc; ESCOFET, Carmen y MORA, Oscar. Software Libre. Bases de datos. Barcelona: Fundació per a la Universitat Oberta de Catalunya, 2005.p.63.
[10] INTERNATIONAL STANDAR ORGANIZATION, Op. cit., p.2.
[11] Ibíd., p.3.
[12] Ibíd., p.3.
[13] Ibíd., p.2.
[14] CISET. Centro de Innovación y Soluciones Empresariales y Tecnológicas. Firewall o cortafuegos. [en línea]. Bogotá: El Sitio [citado 8, enero, 2020]. Disponible en Internet: < URL: https://www.ciset.es/glosario/444-firewall>
[15] INTERNATIONAL STANDAR ORGANIZATION, Op. cit., p.2.
[16] Ibíd., 2.
[17] Ibid., p.2.

engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.[18]

INTEGRIDAD: propiedad de la información relativa a su exactitud y completitud.[19]

NIVEL DE RIESGO: magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad.[20]

POLÍTICA: intenciones y dirección de una organización como se expresan formalmente por la alta dirección.[21]

PROBABILIDAD: oportunidad de ocurrencia de un evento de seguridad de la información. [22]

RIESGO: efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo. La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad.[23]

RIESGO RESIDUAL: riesgo resultante después del tratamiento del riesgo.[24]

VULNERABILIDAD: debilidad de un activo o de control que puede ser explotado por una o más amenazas.[25]

---

[18] KASPERSKY. Ingeniería social. [en línea]. Bogotá: El Sitio [citado 8, enero, 2020]. Disponible en Internet: < URL: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering>
[19] INTERNATIONAL STANDAR ORGANIZATION, Op. cit., p.2.
[20] Ibíd., p.2.
[21] Ibíd., p.2.
[22] Ibíd., p.2.
[23] Ibíd., p.2.
[24] Ibíd., p.2.
[25] Ibíd., p.2.

INTRODUCCIÓN

Actualmente el mundo enfrenta un amplio desarrollo tecnológico del cual surge la necesidad de afrontar grandes retos a nivel de seguridad de la información, es por eso, que la ingeniería ofrece la posibilidad de optar una posición de línea de frente para salvaguardar la información que es de vital importancia para el cumplimiento de sus metas.

Hoy por hoy, lanzar un ataque a una infraestructura tecnológica, no es complejo, si se tiene en cuenta que en internet existen un sin número de herramientas que dan la posibilidad de vulnerar un sistema de información, haciendo que las organizaciones se conviertan en un blanco fácil y atractivo, por eso la importancia de implementar procesos apoyados por un sistema de gestión que permita mitigar, evaluar y contrarrestar eventos de seguridad.

El presente proyecto tiene como fin realizar el diseño de un Sistema de Gestión de Seguridad de la información, para los procesos misionales como la emisión de conceptos, radicación, estudios técnicos, expedición entrega y notificación de licenciamiento urbanístico de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, donde a la fecha no se tiene definido un Sistema de Gestión de seguridad de la Información que apoye y garantice los pilares de la información y que a su vez mitigue las vulnerabilidades que se presenten en la cotidianidad.

Los sistemas de gestión generan orden dentro de un marco organizacional y esto se traducen en valor, lo que significa que las organizaciones, al apoyar sus procesos internos, van a mejorar el desarrollo de sus actividades y a su vez van a mitigar vulnerabilidades que se puedan encontrar presentes dentro del medio donde se desenvuelven granizando la seguridad de la información

El análisis del diseño de Gestión de Seguridad de la Información busca cubrir esas brechas de seguridad, en donde generalmente los directivos, usuarios y demás interesados que conforman la organización, no tienen conciencia sobre los riesgos que corren los activos de información al no tener buenas prácticas y procesos establecidos en el interior de la organización.

Con base a la norma ISO/IEC 27001:2013, se garantiza un tratamiento adecuado para mantener los pilares de la información (integridad, disponibilidad, confidencialidad) dado que estas cualidades protegen la Información, la cual es el activo más valioso para cualquier organización.

Atendiendo lo anteriormente expuesto, el presente documento tiene como fin exponer el diseño de un Sistema de gestión de Seguridad de la Información para la Curaduría urbana No.3 Arq. Ana María Cadena Tobón; para tal fin, se presenta un capítulo dedicado a justificar la propuesta, otro que esboza el problema de investigación, el siguiente muestra los objetivos, posteriormente se enuncia un

marco teórico que sustenta la propuesta, acto seguido se describe el diseño metodológico estructurado en dos fases, a saber: la fase de exploración y la fase de intervención; en la primera se enuncian las subfase de acercamiento a la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón y de diagnóstico; en la segunda se describe la subfase de diseño, que muestra el diseño de un Sistema de Gestión de Seguridad de la información apalancándose en la norma ISO/IEC 27001:2013 y finalmente el documento presenta las conclusiones del ejercicio propuesto.

1. JUSTIFICACIÓN

El sector tecnológico es un área que apoya a todas las áreas económicas en diferentes campos, día a día se puede apreciar que su evolución es cada vez más grande integrándose y convirtiéndose en un área transversal a los objetivos de negocio. No obstante, aunque es un área de vital importancia, al integrar la tecnología con los objetivos de negocio, se tiene que luchar con un paradigma que nace por un desconocimiento por parte de su jerarquía organizacional y que se traduce en "conciencia".

Es una realidad que las organizaciones enfocan sus esfuerzos principalmente en mejorar la productividad o el Core de sus negocios, pero pocas veces hay una conciencia por parte de los Directivos acerca de cómo se debe manejar o qué procesos se deben definir o mejorar a la hora de querer proteger la información o sus activos de información; es por eso, que se deberían cuestionar en todo momento que consecuencia traería si los sistemas de información son vulnerados, si hay un robo de información o si sencillamente se está dando el valor que se requiere al activo más preciado que tiene una organización, la "Información".

Con los avances tecnológicos que se tienen actualmente, realizar un ataque informático o vulnerar un sistema de información resulta muy sencillo dado que no se requiere un amplio conocimiento en sistemas, si no que la facilidad de acceder a la internet da las mismas nociones para utilizar herramientas y así poder realizar un robo de información, o simplemente vulnerar un sistema informático. Kasperky en su boletín de seguridad correspondiente al año 2019 relaciona los siguientes datos estadísticos que sirven como punto de referencia para optar por la implementación de un modelo de seguridad que apunten a las organizaciones y ayuden a garantizar un orden en sus procesos con el fin de salvaguardar sus activos de información y la misma información [26](Ver cuadro 1)

Cuadro 1. Estadísticas boletín de seguridad Kaspersky

BOLETIN DE SEGURIDAD KASPERSKY	
Durante el año, el 19,8% de los equipos de los usuarios de Internet en el mundo sufrieron al menos una vez un ataque web de la clase Malware	AÑO 2019
Los ataques de cifrado se reflejan en 755 485 equipos de usuarios únicos	
Durante el período abarcado por este informe, los criptomineros atacaron a 2 259 038 usuarios únicos	
En 766 728 equipos de los usuarios se neutralizaron intentos de ejecución de programas maliciosos diseñados para robar dinero mediante el acceso en línea a cuentas bancarias	

Fuente. KASPERSKY. Ingeniería social. [en línea]. Bogotá: El Sitio [citado 8, enero, 2020]. Disponible en Internet: < URL: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering>

[26] KASPERSKY, Op. cit., p.2.

De allí nace la necesidad de poder elaborar una propuesta que apunte a diseñar un Sistema de Gestión de Seguridad de la Información para la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, con base en el estándar ISO/IEC 27001:2013, aplicando una metodología de análisis de riesgo.

Teniendo en cuenta lo anterior, es importante destacar que al interior de la organización se abarcan procesos como (Gestión de la información, Gestión administrativa, Gestión Contable, Gestión Institucional, Gestión de atención a usuarios, Sig, Emisiones de conceptos, Radicación, Estudios técnicos, Expedición entrega y notificación, Gestión de la información y TI). Estos procesos ya definidos por la Dirección administrativa de la organización son los que componen el mapa de procesos en su totalidad.

De otro lado, la Curadora Urbana No. 3 Arq. Ana María Cadena Tobón es una persona natural con funciones públicas, elegida por concurso público por el distrito la cual se encarga de expedir las licencias de urbanismo y construcción y otras actuaciones; es allí donde la propuesta de intervención apunta a abarcar los procesos misionales de la organización tales como (Emisión de conceptos, Radicación, Estudios técnicos, Expedición entrega y notificación) los cuales se definen como procesos misionales, dado que es importante asegurar éstos procesos críticos para el Core del negocio. Se busca entonces asegurar como premisa los pilares de la información (integridad, disponibilidad, confidencialidad).

2. PLANTEAMIENTO DEL PROBLEMA

De acuerdo con el antecedente principal identificado, se evidencia que la Curaduría Urbana No.3 de Bogotá Arq. Ana María Cadena Tobón, no cuenta con un Sistema de Gestión de Seguridad de la información para los procesos misionales de la organización.

Al no contar con buenas prácticas no se tienen definidas políticas, procedimientos y controles, lo que ocasiona que los sistemas de información y la información se encuentren expuestos a situaciones que pueden repercutir con la afectación de los objetivos del negocio.

Esta entidad siendo privada con funciones públicas se encuentra regida por entes de control que exigen un nivel de seguridad amplio para el manejo de la información, no obstante esta entidad no cuenta con estrategias de concienciación hacia los usuarios internos, donde esté presente la identificación de riesgos a los cuales se encuentra expuesta la información, adicional a esto, no se tiene seguimiento por medio de revisiones periódicas o planes de mejora continua donde se realicen auditorías internas que validen los mecanismos presentes y aquellos que requieran las mejoras pertinentes.

A partir de este problema de investigación se plantea el siguiente interrogante.

2.1 FORMULACIÓN DEL PROBLEMA

¿Cómo diseñar un Sistema de Seguridad de la Información para la Curaduría Urbana No 3 Arq. Ana María Cadena Tobón de Bogotá en los procesos misionales para el estudio y expedición de licencias urbanísticas y demás actuaciones asociadas?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información, para los procesos misionales de licenciamiento urbanístico y otras actuaciones asociadas de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar el estado actual de la seguridad de la información de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

- Clasificar los activos de información que conforman o pertenecen a la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

- Identificar, gestionar los riesgos presentes en los activos de información de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

- Definir las políticas de seguridad con base en la norma ISO/IEC 27001:2013.

- Diseñar un plan de concienciación para la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

4. MARCO TEORICO

4.1 LA EMPRESA

4.1.1 Antecedentes del Curador Urbano. El decreto 992 de 1996 derogado por el art. 89, Decreto Nacional 1052 de 1998, Por el cual se reglamenta el capítulo IV del decreto extraordinario 2150 de 1995, explica que se suprimen y reforman regulación en cuanto a los procedimientos y trámites innecesarios en la administración pública, y específicamente en el capítulo IV define que los municipios y distritos de más de 100.000 habitantes se dispongan curadores urbanos para que otorguen las licencias de construcción y urbanismo correspondientes de su territorio.[27]

4.1.2 El Curador Urbano. El curador urbano es un particular encargado de estudiar, tramitar y expedir las licencias de urbanismo o de construcción, a petición del interesado en adelantar proyectos de urbanización o de edificación en las zonas de la ciudad que la administración municipal le haya determinado como de su jurisdicción. Igualmente, resolverán las solicitudes de prórroga, revalidación y modificación de dichas licencias. [28]

Los Curadores urbanos son designados por un periodo de 5 años por medio de un concurso de méritos, en los que se elaboran una serie de pruebas de conocimiento específico que se aplica a los aspirantes hecho por el Departamento Administrativo de la Función Pública recibirá el apoyo de la Superintendencia de Notariado y Registro.

Ya elegido Curador la responsabilidad está basada en un ejercicio autónomo, respondiendo disciplinaria, fiscal, civil y penalmente, por todos aquellos daños y perjuicios que se puedan generar a los usuarios, terceros, administración pública y ciudadanía en general. [29]

El propósito principal de elegir una persona con suficiente conocimiento es hacer cumplir las normas urbanísticas haciendo que estos trámites sean especializados y más eficaces que los estudios desarrollados en las oficinas de planeación y cada norma es diseñada para cada municipio o distrito según corresponda.

4.1.3 La Curaduría Urbana. Es la oficina del Curador Urbano, en la cual cuenta con apoyo del grupo interdisciplinario especializado, prestan los servicios de estudio, trámite y expedición de licencias urbanísticas y de construcción.

---

[27] COLOMBIA, CONGRESO DE LA REPUBLICA, Decreto 992 (4, junio, 1996). Por el cual se reglamenta el capítulo IV del decreto extraordinario 2150 de 1995. Bogotá: El Congreso, 1996.p.8.
[28] Ibíd., p.11.
[29] COLEGIO NACIONAL DE CURADORES. ABC del Curador Urbano. [en línea]. Bogotá: El Sitio [citado 11, mayo, 2020]. Disponible en Internet: < URL: https://www.curadoresurbanos.org/abc-del-curador-urbano/>

4.1.4 Marco institucional. La Curaduría Urbana No.3 de Bogotá Arq. Ana María Cadena Tobón: Arq. egresada de la Universidad Nacional de Colombia, Especialista en Derecho Urbano de la universidad del Rosario Administración Financiera de la Escuela de Administración de Negocios y Planeación Territorial de la Universidad de América, La Curaduría Urbana No. 3, está conformada por un selecto grupo de profesionales dispuestos a recibir sus necesidades y realizar el proceso pertinente para convertirlas en soluciones.

Con más de 27 años de ejercicio profesional, Ana María Cadena Tobón se ha desempeñado como la Caradura Urbana No. 3 de Bogotá durante dos periodos comprendidos entre el 12 de septiembre de 2012 y el 11 de septiembre de 2017 y desde el 24 de enero de 2018 hasta la fecha, anteriormente se ha desempeñado en curadurías urbanas como Subdirectora General y Directora Técnica en la empresa privada gestionando principalmente la Dirección de Proyectos y estudios urbanísticos, arquitectónicos y normativos.[30]

4.1.4.1 Productos y servicios. Los productos y servicios que presta la Curaduría Urbana 3 Arq. Ana María Cadena Tobón son:

- Estudio y expedición de Licencias Urbanísticas

- Estudio y expedición de otras actuaciones urbanísticas, como conceptos de norma y uso, propiedad horizontal, movimientos de tierra, entre otros.

- Estudio y expedición de prórrogas y revalidaciones de licencias urbanísticas.

- Asesoría técnica en relación con norma urbana de Bogotá, de sismo-resistencia y ámbito de aplicación del Decreto 1077/15.

- Información a la ciudadanía y/o Entidades Nacionales y Distritales sobre los trámites ejecutados.

4.1.4.2 Stakeholders. Las partes interesadas que intervienen en el proceso de licenciamiento urbanístico son:

- Usuarios: Personas naturales, inmobiliarias, constructoras, tramitadores, Entidades Nacionales y distritales.

- Vecinos y terceros interesados.

[30] CURADURÍA URBANA No. 3. La Curaduría. Disponible desde internet [en línea]. Bogotá: El Sitio [citado 23, agosto, 2020]. Disponible en Internet: < URL: http://curaduria3.com/quienes-somos/curaduria-urbana-no-3/>

- Entidades Nacionales y Distritales: Ministerio de Vivienda, DANE, Alcaldía, Secretaría de Planeación, Secretaría de Hábitat, Secretaría de Hacienda y entes de control como Contraloría, Veeduría, Personería y Procuraduría, Superintendencia de Notariado y Registro.

- Ciudadanía en general.

- Curaduría Urbana.

- Empleados.

4.1.4.3 Direccionamiento estratégico. A continuación, se presenta los componentes del Direccionamiento estratégico

Misión: "Prestar la mejor orientación y servicio a los usuarios en la expedición de licencias urbanísticas y demás actuaciones asociadas, con un equipo humano y profesional con alto sentido de responsabilidad, compromiso, pasión por el trabajo y transparencia, de manera oportuna y efectiva, con el cumplimiento de la normatividad urbanística vigente en la ciudad"[31]

Visión: "Ser la curaduría que marca la diferencia, por ser innovadores en servicio con eficacia, agilidad y confiabilidad. Líderes en metros cuadrados licenciados; con el mejor equipo de trabajo, instalaciones y herramientas tecnológicas".[32]

Principios y valores

- "Transparencia
- Pasión y amor por el trabajo
- Responsabilidad
- Trabajo en equipo
- Respeto
- Compromiso"[33]

Políticas generales

El usuario es la razón de ser de la Curaduría y nuestra gestión se centra en sus necesidades y expectativas

- La actualización normativa al interior de la Curaduría y su divulgación al exterior es prioritaria

[31] Ibid.,p.2.
[32] Ibid.,p.3.
[33] Ibid.,p.2.

- La capacitación permanente de todo el personal en tecnología y en los aspectos relacionados con su oficio, contribuyen a su desarrollo personal

- Nos preocupamos por mantener un buen ambiente de trabajo y generar estímulos y satisfacción a todos nuestros colaboradores.

- En tecnología permaneceremos a la vanguardia.

- Generamos permanentes estrategias de comunicación y posicionamiento en el sector.[34]

Política del Sistema Integrado de Gestión:

Prestar un servicio de estudio y expedición de licencias urbanísticas y demás actuaciones asociadas, logrando la satisfacción de nuestros usuarios y demás partes interesadas a través de:

Compromiso con nuestro Sistema de Gestión de Calidad:

- Prestación de un servicio cálido, cordial y oportuno a través de los diferentes canales de comunicación.
- Planificación, control y mejoramiento continuo de nuestros procesos internos.
- Disminución de los tiempos de respuesta.
- Cumplimiento de la normatividad vigente aplicable.
- Fortalecer las competencias del equipo de trabajo.
- Actualización tecnológica continúa.
- Mantenimiento de instalaciones e infraestructura apropiada.

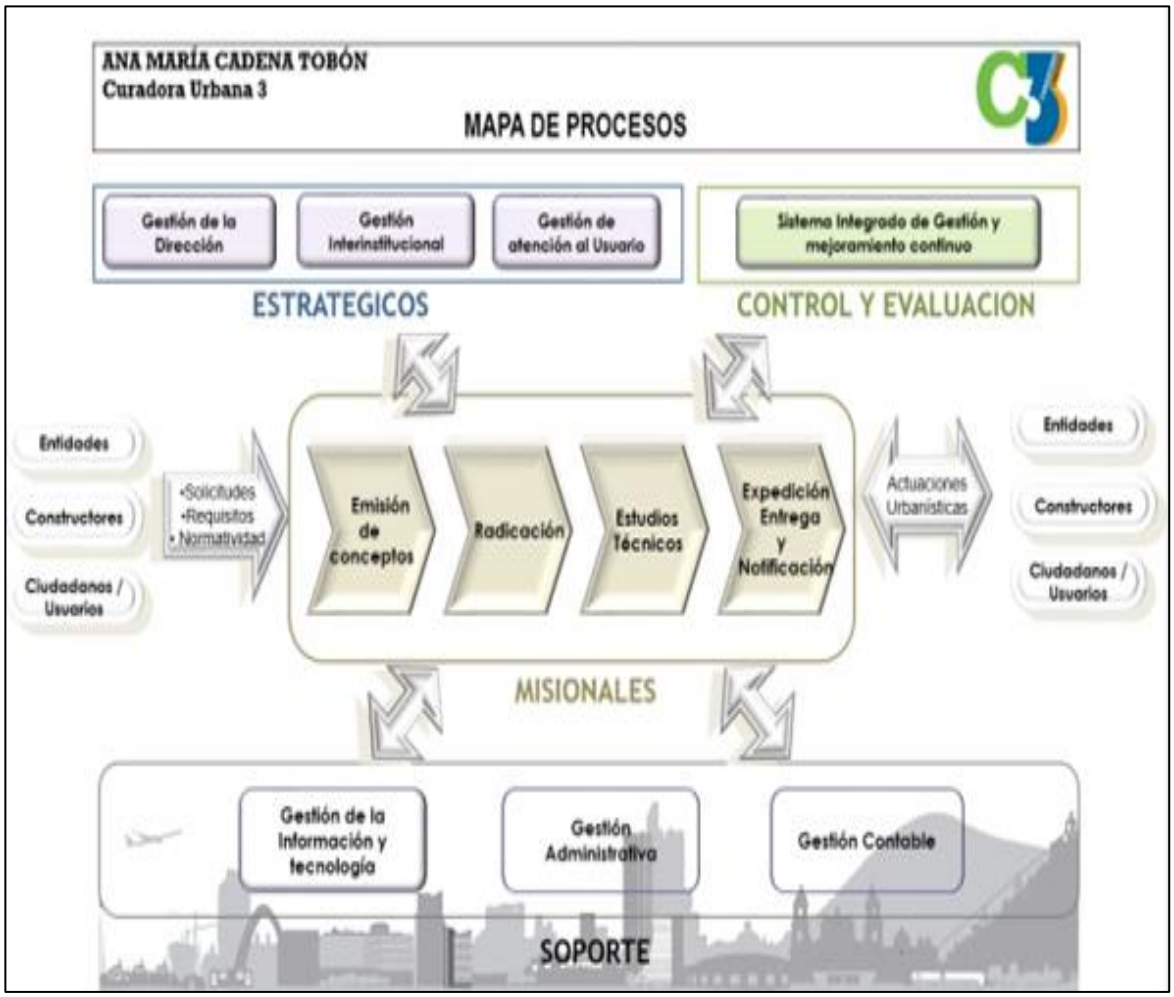
Compromiso con nuestro Sistema de Seguridad y Salud en el Trabajo.

- Generación de condiciones de trabajo seguras y saludables.
- Compromiso con la reducción de peligros y gestión de riesgos.
- Cumplimiento de la normatividad vigente y compromiso con el mejoramiento continuo.
- Compromiso con nuestro Sistema de Gestión Ambiental
- Uso racional y eficiente de los recursos.
- Mitigación impactos ambientales, fomento de protección del medio ambiente y prevención contaminación.
- Cumplimiento de la normatividad vigente y compromiso con el mejoramiento continuo. [35]

[34] Ibid.,p.2.
[35] Ibid.,p.1.

4.1.4.4 Mapa de procesos. A continuación, se presenta el Mapa de Procesos definido para la Curaduría urbana 3 de Bogotá, el cual está conformado por los procesos estratégicos, los procesos de control y evaluación, los procesos misionales y los procesos de soporte. (Ver figura 1)

Figura 1. Mapa de procesos Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.



Fuente: CURADURÍA URBANA No. 3. Documento de Planeación Estratégica. Bogotá: La entidad. 2020.p.12.

4.1.4.5 Estructura organizacional. La planta actual de la curaduría está conformada por 60 personas, estructurada en dos grandes grupos, el primero el equipo de estudios técnicos y el segundo el equipo de gestión operativa y soporte (ver cuadro 2)

Cuadro 2. Estructura organizacional

CURADOR URBANO	
Área Técnica	**Área Administrativa y de Gestión**
Arquitectura	Área de Información y Tecnologia
Ingenieria	
Juridica	Área Administrativa
Consultas ,Conceptos y Zonificación	Área de Contabilidad
	Sistema integrado de Gestión
33 Personas	**27 personas**
Total 60 personas	

Fuente: CURADURÍA URBANA No. 3. Informe Final de Gestión. Bogotá: La entidad. 2017.p.6.

4.1.5 Definición de los procesos de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón. Dentro de su composición la Curaduría Urbana No.3 ha definido los procesos que enmarca dicha institución, estos se visualizan en la figura 2. y su objetivo tiene como directriz ofrecer la calidad organizacional, estos son comprendidos en 4 grupos.

Proceso estratégico: este grupo es el encargado de todo el planeamiento institucional, su principal función es la dirigir y a la vez apoyar otros procesos que componen la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón. este está conformado por:

- Gestión de la Dirección.
- Gestión Interinstitucional.
- Gestión de atención al usuario.

Proceso de control y evaluación: su principal función va orientada a brindar un apoyo en ejercicio al control y a la evaluación para obtener así mediciones con relación al progreso de objetivos trazados. Este está conformado por el Sistema integrado de gestión y mejoramiento continuo.

Procesos misionales: este proceso es el encargado de realizar una trasformación de cara a los usuarios que hacen uso del servicio que presta la entidad recibiendo un producto.

- Emisión de conceptos.
- Radicación.
- Estudios técnicos.
- Expedición entrega y notificación.

Proceso de soporte: El proceso de soporte es el encargado de apoyar y gestionar

los procesos misionales de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

- Gestión de la información y la Tecnología.
- Gestión Administrativa.
- Gestión Contable.

Lo anterior se resume en la figura 2

Figura 2. Procesos misionales Curaduría Urbana No. 3

Fuente: CURADURÍA URBANA No. 3. Documento de Planeación Estratégica. Bogotá: La entidad. 2020.p.12.

4.1.6 Procesos misionales. Los procesos misionales de la Curaduría Urbana 3 Arq. Ana María Cadena Tobón son:

- **Proceso emisión de conceptos:** planifican las actividades necesarias para la oportuna elaboración y entrega de los conceptos de uso, reparaciones locativas o de norma que, solicitados por los usuarios, según aplique.

- **Proceso de radicación:** esta área de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón es la responsable de recibir y verificar la documentación suministrada por el usuario para su radicación, de acuerdo al tipo de trámite a desarrollar. Inicia desde el recibo de la solicitud del usuario y termina con el alistamiento del expediente y descarga para inicio de estudio.

- **Proceso de estudios técnicos**: desarrollan las actividades necesarias para el estudio Arquitectónico, estructural y jurídico de las solicitudes licencias urbanísticas y demás actuaciones asociadas radicadas en la Curaduría.

- **Procesos de expedición entrega y notificación:** gestionan las actividades de expedición de los actos administrativos generados por la Curaduría Urbana No. 3 hasta su ejecutoria.

4.2 SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es un conjunto de directrices definidas que se utilizan para minimizar los riesgos a los que se exponen los activos de información dentro de una Curaduría Urbana N.3 Arq. Ana María Cadena Tobón, su objetivo principal es proteger y asegurar las cualidades de la información (Confidencialidad, integridad y disponibilidad) de tal modo que se pueda mitigar cualquier evento que vulnere estas cualidades. La seguridad de la información va acompañada de estrategias que apunta a cubrir las necesidades existentes en donde se debe salvaguardar el activo más preciado, la información.

- **Confidencialidad:** este principio establece que la información solo debe ser accedida a personas o componentes que cuenten con una previa autorización.

- **Integridad*:*** su objetivo principal es garantizar que la información esté libre de cualquier modificación no autorizada, garantizando de este modo que la información se mantenga exacta como fuente original generada.

- **Disponibilidad*:*** garantiza que la información este siempre disponible cuando se requiera para ser utilizada por personas, entidades, o procesos que se encuentren debidamente autorizados.

4.3 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Un sistema de gestión de seguridad de la información se define como “el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una Curaduría Urbana N.3 Arq. Ana María Cadena Tobón, en la búsqueda de proteger sus activos de información esenciales”[36]

“Un SGSI desde la visión del estándar internacional ISO/IEC 27001:2013 es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una Curaduría Urbana N.3 Arq. Ana María Cadena Tobón y lograr sus objetivos comerciales y/o de servicio.”[37]

4.4 NORMA ISO/IEC 27001:2013

Esta norma es de carácter internacional y fue avalada y publicada por la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón de normalización ISO/IEC 27001:2013

---

[36] CURADURÍA URBANA No. 3. Documento de Planeación Estratégica. Bogotá: La entidad. 2020.p.12.

[37] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO-IEC 27001. Bogotá, D.C.: El Instituto, 2006. p. 3.

con el propósito de “suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información”[38]además “puede ser usada por partes internas y externas para evaluar la capacidad de la organización para cumplir los requisitos de seguridad de la propia organización.”[39]Su composición “incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización.”[40]Esta norma no excluye un tipo de organización específico, por el contrario, se puede aplicar a cualquier contexto organizacional, los apartados que compones esta norma son los siguientes:

- Objeto y campo de aplicación.
- Referencias y normativas.
- Términos y definiciones.
- Contexto de la organización.
- Liderazgo.
- Planificación.
- Soporte.
- Operación.
- Evaluación de desempeño.
- Mejora.

4.5 NORMA ISO 27002

Esta norma es un código de practica en donde:

> Se establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización los objetivos indicados en esta norma brindan una guía sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información. Los objetivos de control y los controles de esta norma están destinados a ser implementados para satisfacer los requisitos identificados por la evaluación de riesgos [41]

Por lo general esta guía se opta para seguir lineamientos al momento de desarrollar normas que de seguridad que se apliquen a la organización dando como valor la creación de confianza.

---

[38] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO-IEC 27001. Bogotá, D.C.: El Instituto, 2006. p. i.
[39] Ibíd., p.1.
[40] Ibid., p.2.
[41] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Tecnología de la Información. Técnicas de seguridad. Tecnología de la información técnicas de seguridad. Código de practica para la gestión de la seguridad de la información. Objeto. NTC-ISO-IEC 27002. Bogotá, D.C.: El Instituto, 2007. p. 1.

4.6 NORMA ISO 27003

Esta norma se toma como una guía cuyo objeto tiene como propósito la validación en donde:

> Enfoca en los aspectos críticos necesarios para el diseño e implementación exitosos de un Sistema de Gestión de la Seguridad de la Información (SGSI) de acuerdo con la norma ISO/IEC 27001:2013. En la misma se describen los procesos de especificación y diseño de un SGSI, desde el inicio hasta la producción de los planes de implementación, esta guía está prevista para ser usada por organizaciones que se encuentren implementando un SGSI. Es aplicable a todos los tipos de organizaciones (por ejemplo, empresas comerciales, organismos gubernamentales, organizaciones sin fines de lucro) de cualquier tamaño. La complejidad y los riesgos de las organizaciones son únicos, y sus requisitos específicos dirigirán la implementación del SGSI[42]

Por lo anterior esta norma es utilizada como apoyo para una óptima implementación.

4.7 NTC-ISO 31000

La ISO 31000 nos "brinda los principios y las directrices genéricas sobre la Gestión del riesgo"[43]. Así mismo esta norma "puede ser utilizada en cualquier empresa pública o comunitaria asociación, grupo o individuo."[44]

En la ISO 31000 "en esta se usan las expresiones "Gestión del riesgo" y "gestionar el riesgo". En términos generales, la Gestión del riesgo se refiere a la "Arquitectura (principios, marco y procesos) para la gestión eficaz del riesgo, mientras que Gestionar el riesgo se refiere a la aplicación de esa Arquitectura a riesgos particulares"[45].

Ahora bien, teniendo en cuenta que la ISO 31000 trabaja sobre la gestión del riesgo se determina que "el éxito de la Gestión del riesgo dependerá de la eficacia del marco de referencia para la Gestión, el cual brinda las bases y las disposiciones que se introducirán en todos los niveles de la organización."[46]

---

[42] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Tecnología de la Información. Técnicas de seguridad. Guía de implementación de un sistema de gestión de la seguridad de la información. Objeto. NTC-ISO-IEC 27003. Bogotá, D.C.: El Instituto, 2012. p. 1.

[43] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACION (ICONTEC). Gestión del riesgo. Principios y directrices. NTC-ISO 31000:2009. [en línea]. Bogotá, D.C.: El Instituto, 2011. p. 3.

[44] Ibíd. p.3.

[45] Ibíd., p.2.

[46] Ibíd., p.3.

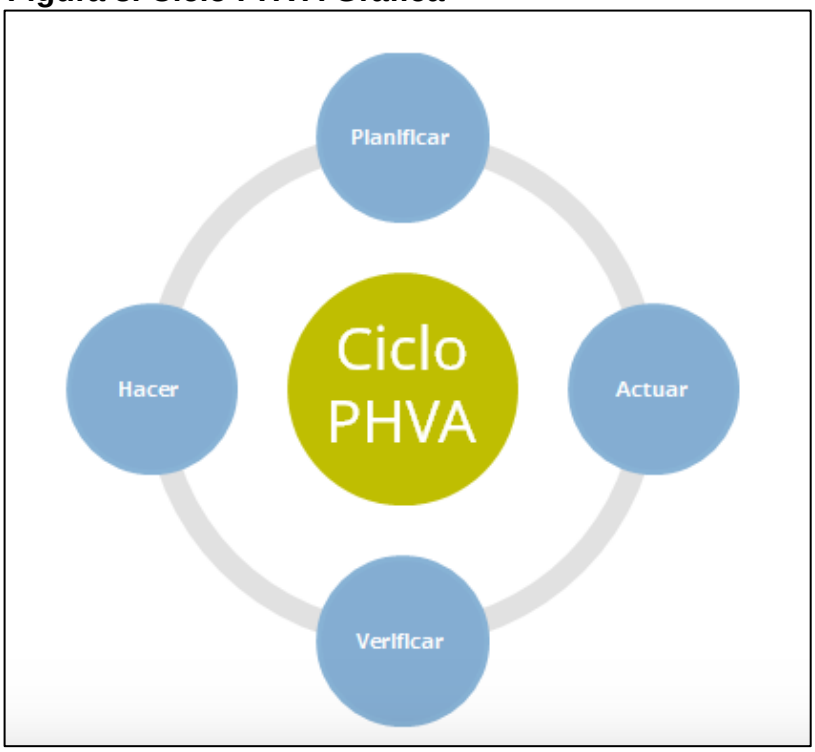
4.8 CICLO PHVA

Para llevar a cabo la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma internacional ISO/IEC 27001:2013, se debe utilizar el ciclo PDCA (siglas en inglés) o PHVA (siglas en español). (Ver figura 3).

Dicho ciclo cuenta con los siguientes pasos:

- "Planificar*:* se establece el Sistema de Gestión de Seguridad de la Información.
- Hacer*:* se implementa el SGSI.
- Verificar*:* se revisa el Sistema de Gestión de Seguridad de la Información.
- Actuar: mantener y mejorar el SGSI."[47]

Figura 3. Ciclo PHVA Grafica



Fuente: ISOTOOLS. ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información mediante el ciclo PHVA, Norma ISO 27001. [en línea]. España: El Sitio [citado 23, agosto, 2020]. Disponible en Internet: < URL: https://www.isotools.pe/iso-27001-implementacion-sistema-gestion-seguridad-informacion-ciclo-phva/>

[47]ISOTOOLS. ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información mediante el ciclo PHVA, Norma ISO 27001. [en línea]. España: El Sitio [citado 23, agosto, 2020]. Disponible en Internet: < URL: https://www.isotools.pe/iso-27001-implementacion-sistema-gestion-seguridad-informacion-ciclo-phva/>

5. DISEÑO METODOLÓGICO

El diseño metodológico que contiene la propuesta esta permeado por las siguientes características:

- **Universo poblacional:** la propuesta de intervención se realizará en la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, ubicada en la localidad de Barrios Unidos en la ciudad de Bogotá; la aplicación de esta propuesta se aplicará directamente a los procesos misionales organizativos (Emisión de conceptos, Radicación, Estudios Técnicos, Expedición entrega y Notificación).

- **Objeto o unidad de análisis:** la propuesta centra su estudio en el diseño de un sistema de gestión de seguridad de la información para la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

- **Técnicas e instrumentos de recolección de la información:** la información obtenida en la propuesta se recogerá a través del instrumento de encuesta que permite recolectar los conocimientos de los funcionarios que hacen parte de los procesos misionales de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón en relación con la seguridad de la información.

La propuesta se desarrollará en 2 fases, una de exploración y la otra de intervención, en cada una se presenta una descripción de las acciones ejecutadas, seguida del análisis y las reflexiones de dichas acciones apoyadas desde los instrumentos de medición y bajo los controles de la norma ISO/IEC 27001:2013.

5.1 FASE DE EXPLORACIÓN

La fase de exploración determina el estado inicial de la seguridad de la información de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón. Para su desarrollo esta fase se divide en dos subfases,

5.1.1 Subfase de acercamiento a la organización. En esta subfase se realizó un acercamiento con la Dirección Administrativa de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón con el objetivo de socializar la propuesta de intervención y así conocer los procesos misionales más en detalle para tener una visión y un panorama que permita entender su Core de negocio y como éste interactúa con la norma ISO/IEC 27001:2013 en un escenario actual. Para ello se realizaron las siguientes actividades en orden cronológico.

- Visita a las instalaciones de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

- Reunión con la Dirección de la Curaduría Urbana N.3 Arq. Ana María Cadena

Tobón (Anexo A).

- Entrevista con líderes de proceso (Anexo B)
- Entrevista con Departamento de Tecnología (Anexo C) .

Se realizó un acercamiento primario por medio de uno de los integrantes autores de la presente propuesta de intervención con la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón, allí se interactuó con la Dirección Administrativa quien en primera estancia escucho la propuesta avalando la intervención y autorizando el ingreso a la sede por parte del otro integrante autor de la propuesta para visitar la sede y realizar la aplicación de instrumentos de medición.

5.1.2 Subfase de diagnóstico. Durante esta súbase se elaboró un cronograma de reuniones con los líderes de procesos en donde se socializó la aplicación de un cuestionario ISO/IEC 27001:2013 dirigido a la Gerencia y la Coordinadora Administrativa y SIG y una encuesta a los funcionarios que hacen parte de los procesos misionales para indagar el estado actual de la Curaduría Urbana No. 3 Arq. Ana María Cadena Tobón en relación con la Seguridad de la Información.

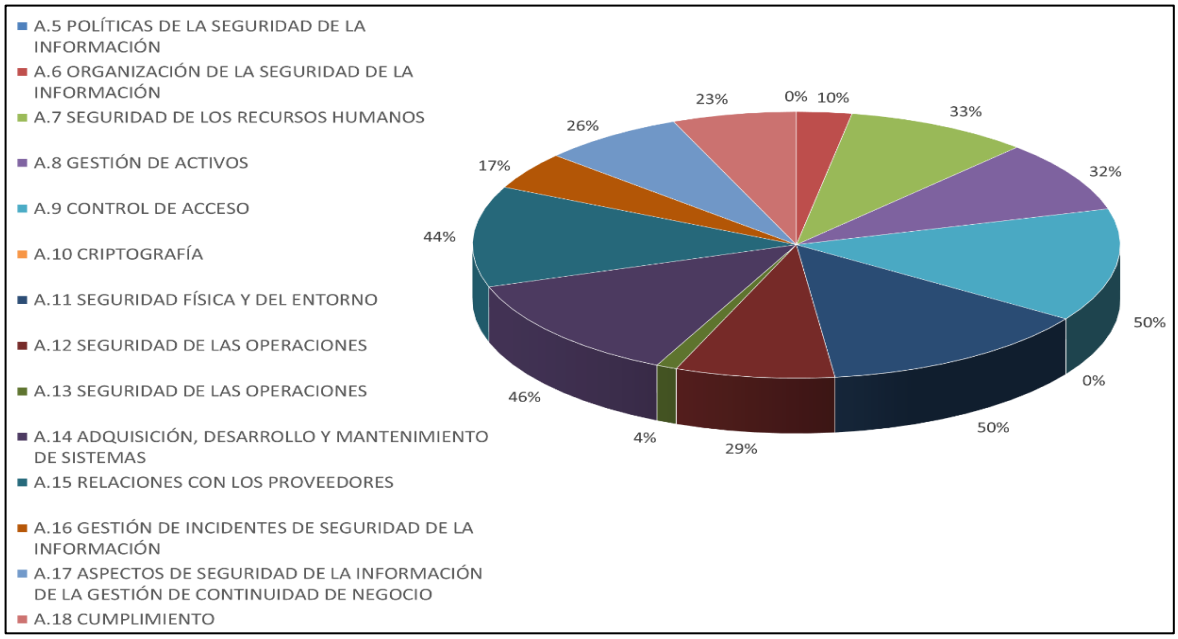
Uno de los instrumentos utilizados para realizar el sondeo con la gerencia fue el cuestionario ISO/IEC 27001:2013 donde se tienen en cuenta los controles de la norma ISO/IEC 27001:2013 y para la realización de la encuesta a los funcionarios se hizo uso de la herramienta Google Forms con un formulario de 18 preguntas cerradas publicado en el sitio web:
https://docs.google.com/forms/d/1ZIjDcELkpd5DIIWp_-ktejXu96wrratUCZby1vhsgkA/edit

A continuación, se describen los resultados del cuestionario, la encuesta, y la triangulación de los dos instrumentos, seguida del análisis de resultados a la luz de la reflexión.

5.1.2.1 Resultados diagnóstico. Resultados y análisis del cuestionario ISO/IEC 27001:2013 aplicado a la gerencia y la Coordinadora Administrativa y SIG.

Se elaboró diagnóstico completo que comprende los diferentes dominios de la norma ISO/IEC 27001:2013 diligenciado por la Gerencia y la Coordinadora Administrativa y SIG que muestra los siguientes resultados. El diagnostico puede evidenciarse en el (Anexo E).

Gráfica 1. Estado Inicial de la Curaduría Urbana No. 3 - General.



Fuente: Los Autores

En la gráfica 1 se evidencia que la Curaduría Urbana 3. Arq. Ana María Cadena Tobón, aunque no tiene implementado un SGSI presenta un avance significativo con relación a los subdominios que la norma ISO/IEC 27001:2013 define, este avance corresponde al 26%.

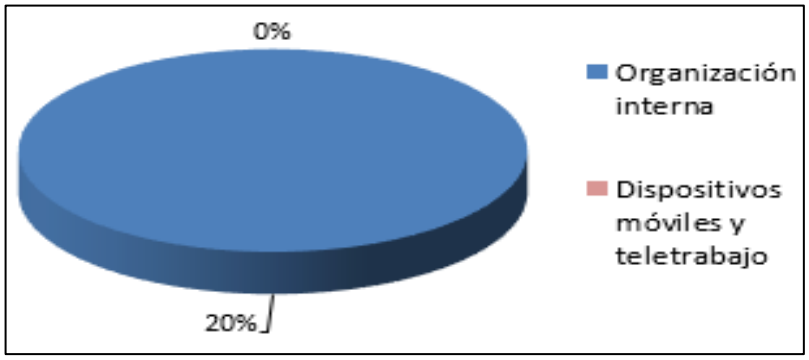
Dando continuidad al a la aplicación del instrumento de medición, a continuación, se muestran los resultados obtenidos con relación a los controles de la norma ISO/IEC 27001:2013

Gráfica 2. Estado inicial de la Curaduría Urbana No. 3 Políticas de la seguridad de la información

Fuente: Los Autores

La gráfica 2 define que la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón no cuenta con políticas de seguridad de la información definidas lo que conlleva en que no se cuente con una orientación por parte de la alta Dirección para apoyar su cumplimiento.

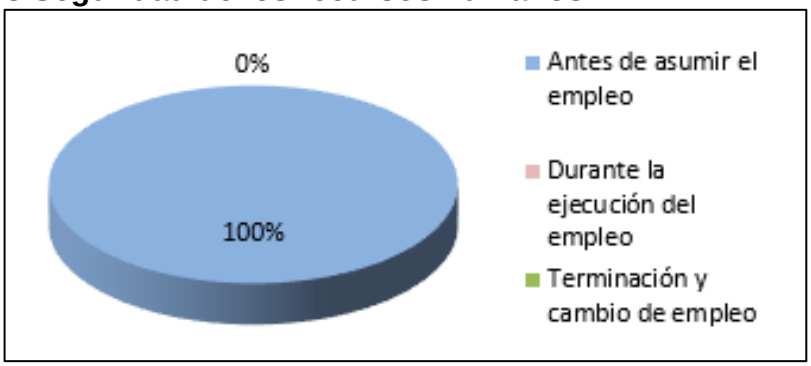
Gráfica 3. Estado actual de la Curaduría Urbana No. 3



Fuente: Los Autores

La gráfica 3 muestra que la Curaduría Urbana 3. Arq. Ana María Cadena Tobón cuenta con un avance en relación al modo de conformación en validación a las responsabilidades que se tiene internamente, para ello se define un porcentaje del 20%, no obstante, no se contemplan mecanismos que permitan tener una cobertura para dispositivos móviles o modalidades de teletrabajo lo que relaciona un porcentaje de implementación del 0%, es importante tener en cuenta que por la nueva normalidad es de vital importancia contar con una cobertura a dispositivos y modalidades de apoyo que permitan garantizar la seguridad de la información .

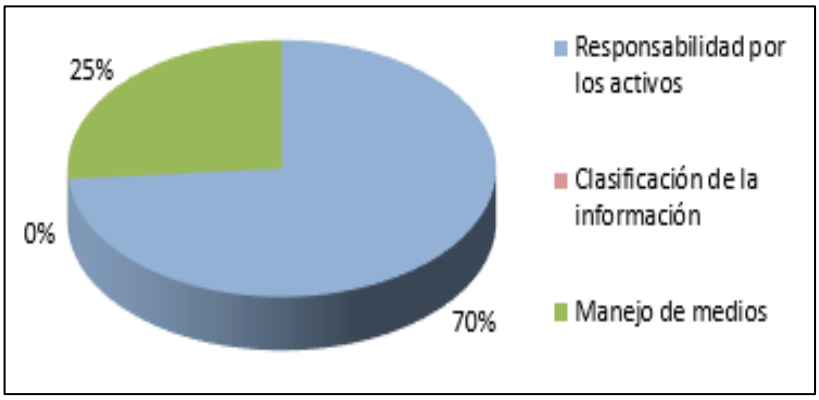
Gráfica 4. Estado actual de la Curaduría Urbana No. 3 Seguridad de los recursos humanos



Fuente: Los Autores

La gráfica 4 evidencia que la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón cuenta con procesos definidos en relación a la selección del personal para ejecución de los cargos, antes de asumir el empleo, estos acuerdos se realizan haciendo uso de mecanismos contractuales lo que conlleva a un porcentaje de implementación del 100%, durante la ejecución del empleo no se cuenta, con programas de formación y capacitación en relación a la seguridad de la información, del mismo modo tampoco se hace claridad al empleado sobre sus responsabilidades en relación a la seguridad de la información luego de culminar o cambiar su contrato en calidad de empleado, por lo anterior su porcentaje de implementación corresponde al 0%

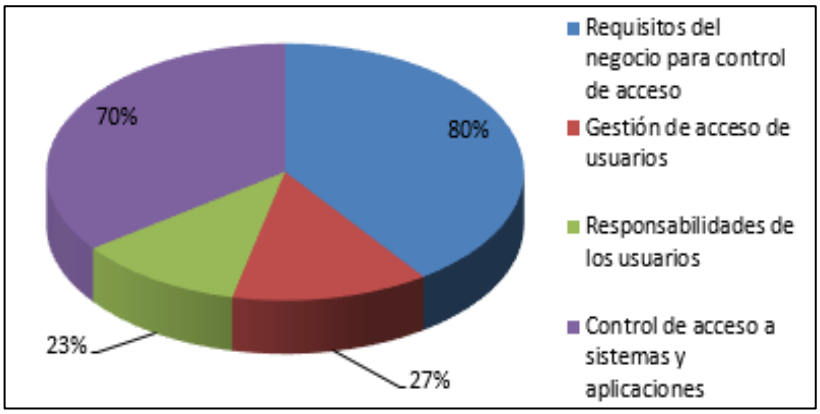
Gráfica 5. Estado actual de la Curaduría Urbana No. 3 Gestión de activos



Fuente: Los Autores

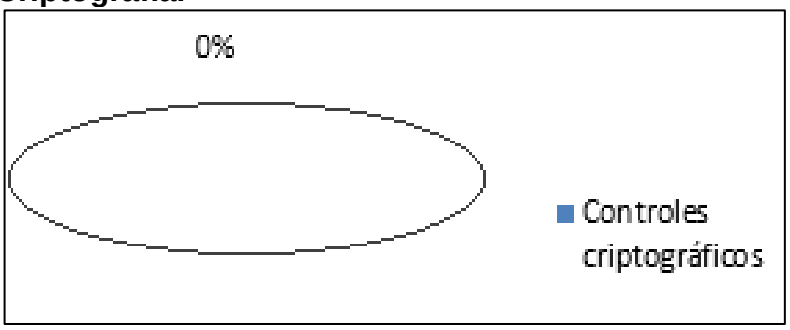
En la gráfica 5 se muestra que en relación a la gestión activos se evidencia que la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón se esmera por gestionar sus activos de manera adecuada esto nos da como resultado el 70% en la responsabilidad por los activos, no obstante, no se tiene definido un procedimiento en donde se evidencie de manera clara y precisa el responsable y el manejo del activo, tampoco se encuentra etiquetado lo que conlleva a un porcentaje de implementación del 0 %, en el manejo de medios se tiene una restricción a los medio para la seguridad pero esto hace que la disposición de los medios y el manejo adecuado de los activos no se lleve a cabo ya que se tiene restringido mas no controlado esto hace que la calificación en el cumplimiento sea de un 25%

Gráfica 6. Estado actual de la Curaduría Urbana No. 3 Control de acceso



Fuente: Los Autores

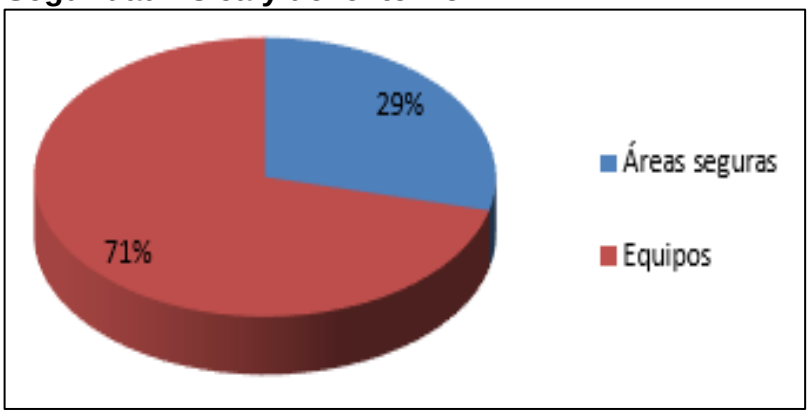
Gráfica 7. Estado actual de la Curaduría Urbana No. 3 Criptografía.



Fuente: Los Autores

En la gráfica 7 muestra que no se cuenta con la creación y uso estricto de políticas definidas en cuanto a controles criptográficos esto da el porcentaje de implementación es del 0%

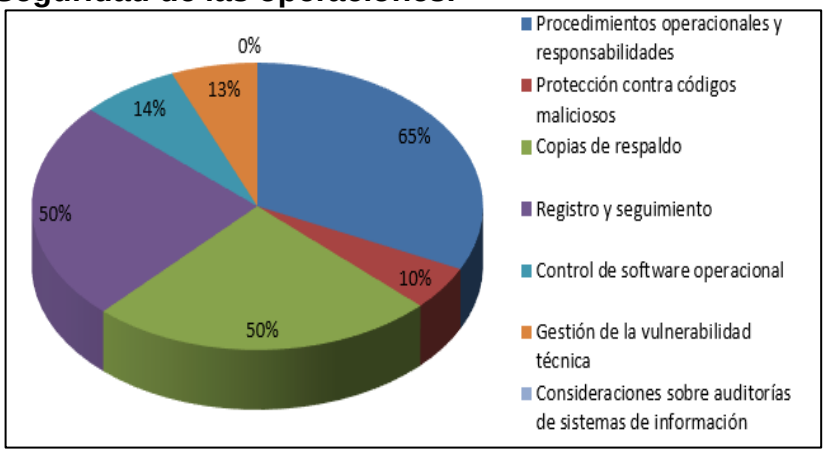
Gráfica 8. Estado actual de la Curaduría Urbana No. 3 Seguridad física y del entorno



Fuente: Los Autores

La gráfica 8 muestra que la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón cuenta con un porcentaje del 29% en relación con la definición de áreas seguras donde reposan los activos de información, aunque no se tengan definidos procedimientos a nivel de equipos se relaciona un porcentaje del 71% teniendo en cuenta que se debe mejorar la atención a equipos desatendidos y se debe implementar una política de escritorio limpio, lo que se estima implementar con el diseño del SGSI

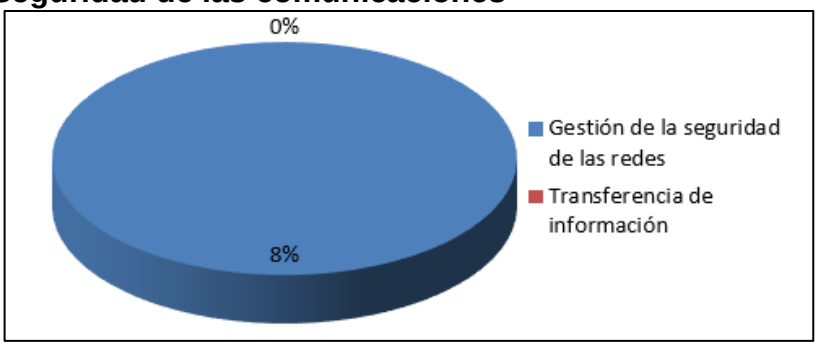
Gráfica 9. Estado actual de la Curaduría Urbana No. 3 Seguridad de las operaciones.



Fuente: Los autores

La gráfica 9 muestra los resultados correspondientes a la seguridad en operaciones que arroja como resultado 65% en procedimientos operacionales y responsabilidades, se evidencia que hace falta implementación de controles de acceso físicos, gestión de capacidad hacia proyecciones futuras, un 10% de implementación en la protección contra códigos maliciosos dado a que hace falta la gestión en la capacidad de recuperación, un 50% en las copias de respaldo realizadas por la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón porque se realizan las copias pero no se cuenta con política definida para la realización de las mismas, un 50% en el registro y seguimiento dado a que se registran los eventos pero no se tiene un responsable del evento, un 14 % en el control de software operacional porque hacen falta procedimientos para la instalación de software, un 13% en gestión de la vulnerabilidad técnica porque no se obtiene información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información y un 0% en las consideraciones sobre auditorías de sistemas de información porque no se tienen en cuenta en la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón para identificar las interrupciones en los procesos del negocio.

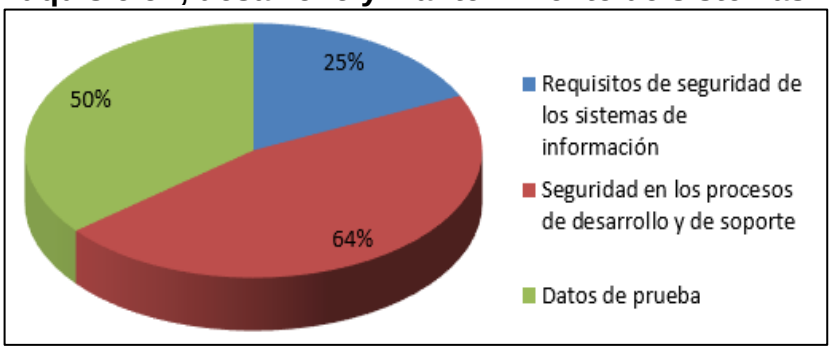
Gráfica 10. Estado actual de la Curaduría Urbana No. 3 Seguridad de las comunicaciones



Fuente: Los autores

En la gráfica 10 se evidencia un cumplimiento parcial del 8% en relación a la gestión de la seguridad de las redes teniendo en cuenta que la infraestructura cuenta con una protección haciendo uso de Antivirus, Firewall y esta se encuentra segmentada , sin embargo hace falta la implementación de ANS o tiempos de respuesta que permitan tener una respuesta oportuna en tiempos de caída de los servicios, adicional a lo anteriormente expuesto se debe definir los acuerdos de trasferencia de información entre las partes interesadas, finalmente se debe velar por la socialización de los acuerdos de confidencialidad requeridos.

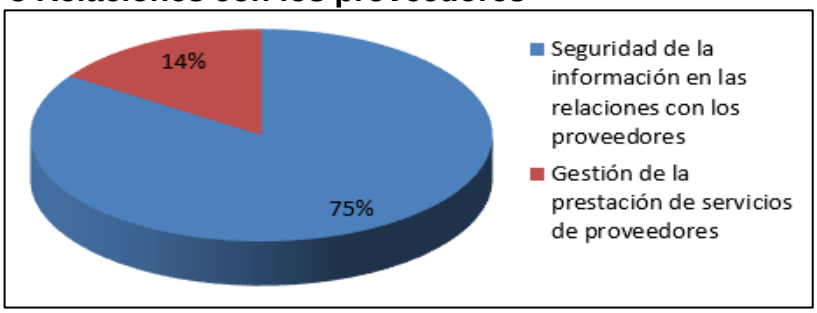
Gráfica 11. Estado actual de la Curaduría Urbana No. 3 Adquisición, desarrollo y mantenimiento de sistemas



Fuente: Los autores

En la gráfica 11 se relaciona como resultado el 25% de cumplimiento en los requisitos de seguridad de los sistemas de información porque no están incluidos en las mejoras de los sistemas; el 64% de cumplimiento en la seguridad de los procesos de desarrollo y de soporte en donde se evidencio la falta de políticas de desarrollo seguro, procedimientos de control de cambios en sistemas, no se realiza revisión técnica de las aplicaciones después de cambios en la plataforma de operación, no se cuenta con un ambiente de desarrollo seguro, no se discriminan principios de construcción de los sistemas seguros; el 14% de cumplimiento en datos de prueba es generado debido a que no se establecen programas de prueba para aceptación y criterios para los sistemas.

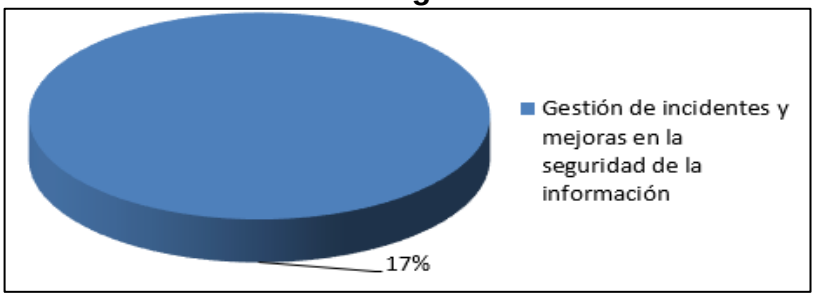
Gráfica 12. Estado actual de la Curaduría Urbana No. 3 Relaciones con los proveedores



Fuente: Los autores

En la gráfica 12 se evidencia un porcentaje del 75% en validación a la seguridad de la información en las relaciones con los proveedores dado a que la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón de cierta manera busca hacer partícipe a los proveedores sobre los procesos a los que apoya con la prestación de un servicio, sin embargo el 14% restante obedece a factores como la gestión de cabios de suministro por parte de proveedores en lo que hace falta trabajar con el fin buscar un afinamiento en la mejora oportuna de este de prestaciones de servicio.

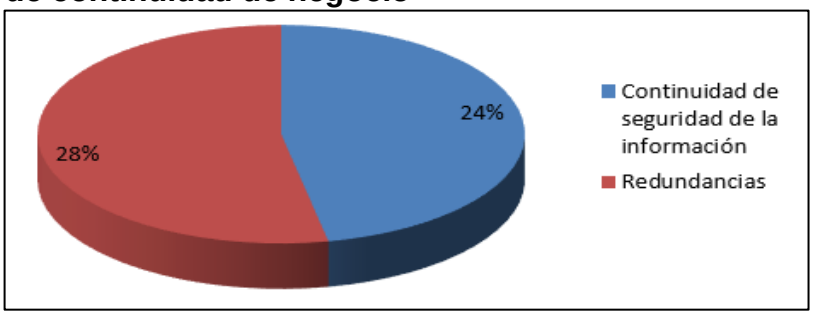
Gráfica 13. Estado actual de la Curaduría Urbana No. 3 Gestión de incidentes de seguridad de la información



Fuente: Los autores

En la gráfica 13 se evidencia un porcentaje del 17% que corresponde la calificación general de la gestión de incidentes de seguridad de la información porque no se cuenta con procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

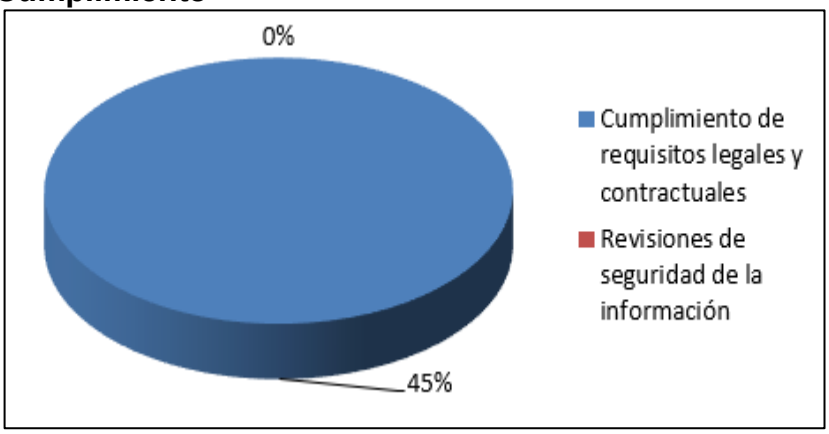
Gráfica 14. Estado actual de la Curaduría Urbana No. 3 Aspectos de seguridad de la información de la gestión de continuidad de negocio



Fuente: Los autores

En la gráfica 14 se evidencia que 24% dado a que la operación está en marcha en un día a día, no obstante no se tiene definidos controles que permitan tener una continuidad en seguridad de la información, cuando estos controles existan se debe verificar la eficacia de estos, seguidamente se debe buscar un afincamiento en relación a buscar una mejora en la redundancia en las unidades de almacenamiento lo que garantice la disponibilidad, por tal motivo esta redundancia se evidencia con un porcentaje de implementación del 28%.

Gráfica 15. Estado actual de la Curaduría Urbana No. 3 Cumplimiento



Fuente: Los autores

En la gráfica 15 se evidencia que el 23% de los controles de cumplimiento se encuentran implementados tales como los derechos de propiedad intelectual, la protección de registros, la protección de datos personales, pero se tienen deficiencias en que no se revisan independientemente los temas relacionados a la seguridad de la información, no se cumplen con las normas de seguridad ya que no se tienen políticas para las mismas.

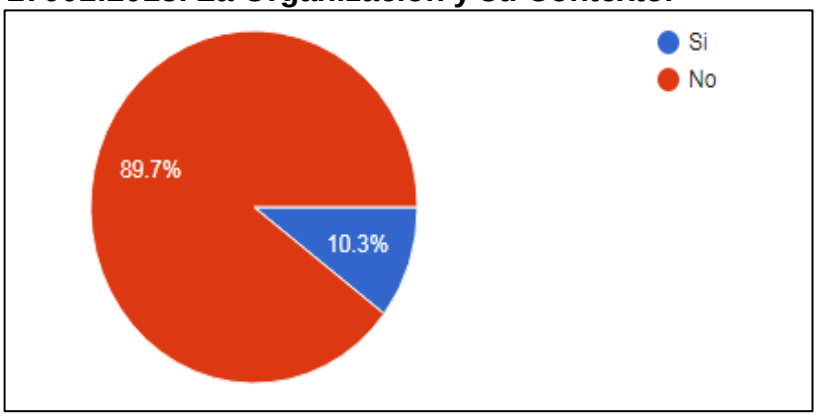
- **Resultados y análisis de la encuesta aplicada a los funcionarios de los procesos misionales.** Con base en la idea de un SGSI se elaboró un cuestionario por medio de la herramienta Google Forms de 18 preguntas para distribuir por medio de correo electrónico a los funcionarios que hacen parte de los procesos misionales al interior de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

- **Selección de funcionarios** Se aplicó la encuesta a 30 funcionarios de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón que hacen parte de los procesos misionales en la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón. Esta encuesta inicial describía 18 preguntas cerradas, Se aplicó a partir de una herramienta de análisis de brecha llamada test de cumplimiento ISO/IEC 27001:2013 y tomada del sitio de la referencia ISO/IEC 27001:2013, la cual se aplicó a cargos que se encuentran desarrollando un procedimiento en los procesos misionales de la Curaduría.

- **Recolección de datos.** Una vez los funcionarios participaron activamente de la encuesta, se recogieron los datos y se analizaron mostrando los siguientes resultados:

- ¿Están identificados los objetivos del "SGSI" Sistema de Gestión de la Seguridad de la Información?

Gráfica 16. Test de Cumplimiento Norma ISO/IEC 27001:2013. La Organización y su Contexto.

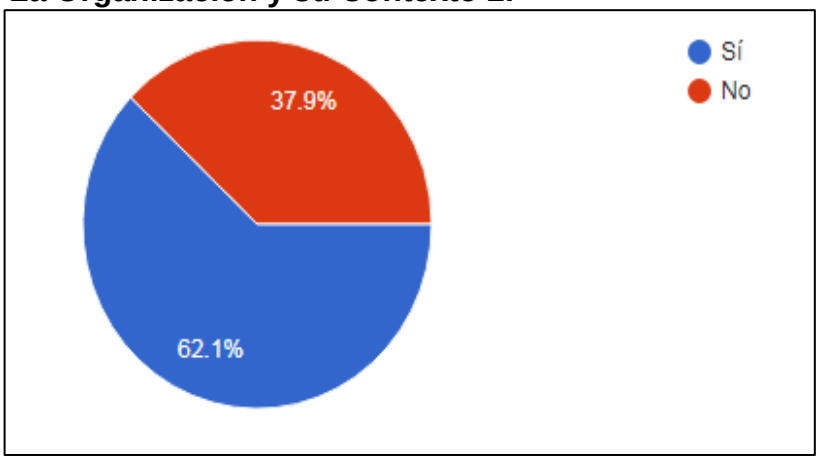


Fuente: Los autores

La gráfica 16 evidencia que el 89.7% de las personas encuestadas NO identifican los objetivos del SGSI y el 10.3% dice que SI, lo anterior obedece a que el 89.7% posiblemente no tenga claridad sobre que es un SGSI y cuál es el propósito de su implementación.

- ¿Existen requisitos sobre Seguridad de la información de las partes interesadas?

Gráfica 17. Test de Cumplimiento Norma 27001:2013. La Organización y su Contexto 2.

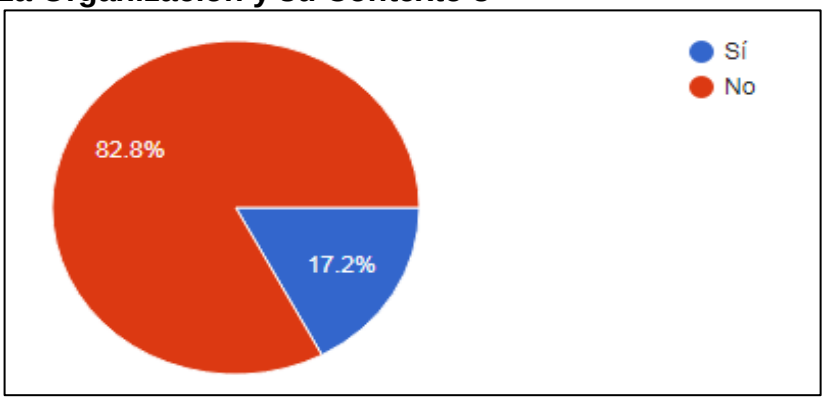


Fuente: Los autores

En la gráfica 17 se evidencia que el 62.1% de las personas encuestadas dice que SI existen requisitos sobre seguridad de la información y el 37.9% dice que NO, lo anterior porque no se tiene claro que partes actúan directamente con el SGSI.

- ¿La Curaduría Urbana N.3 Arq. Ana María Cadena Tobón cuenta con un sistema de seguridad de la información?

Gráfica 18. Test de Cumplimiento Norma 27001:2013. La Organización y su Contexto 3

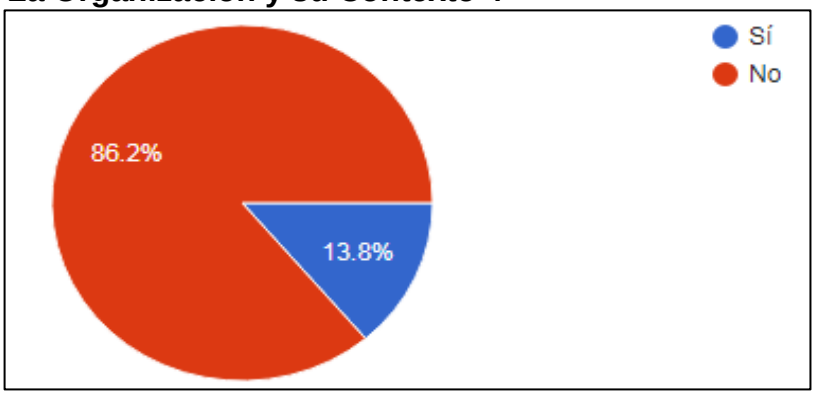


Fuente: Los autores

La gráfica 18 evidencia que el 82.8% dice que la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón NO cuenta con un sistema de seguridad de la información y el 17.2% dice que SI, lo anterior obedece a que 82.8% de los usuarios tiene una idea sobre que es SGSI identificando algunos componentes y el 17.2% manifiesta que si esta implementado en su totalidad el SGSI, pero no tienen claridad cuáles son todos los componentes que hacen parte de un SGSI.

- ¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?

Gráfica 19. Test de Cumplimiento Norma 27001:2013. La Organización y su Contexto 4

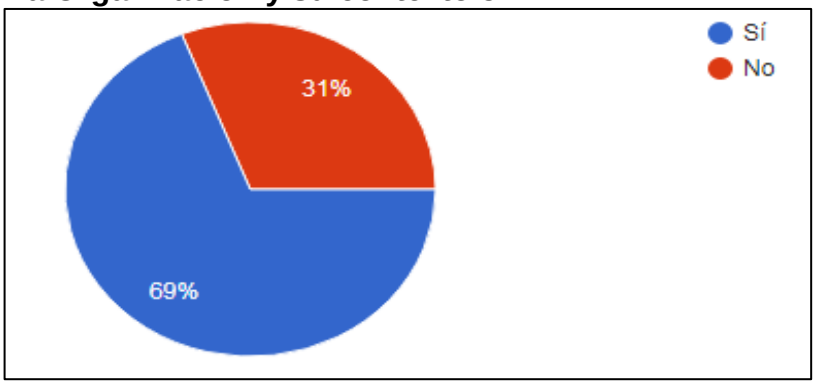


Fuente: Los autores

Rn la gráfica 19 se muestra que el 86.2% dice que el sistema de Gestión de Seguridad de la información NO está establecido implementado y el 13.8% dice que SI, lo anterior obedece a que porque no se tiene claridad sobre una definición exacta de Sistema de Seguridad de la Información y que componentes se tiene implementados de manera parcial.

• ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?

Gráfica 20. Test de Cumplimiento Norma 27001:2013. La Organización y su contexto 5

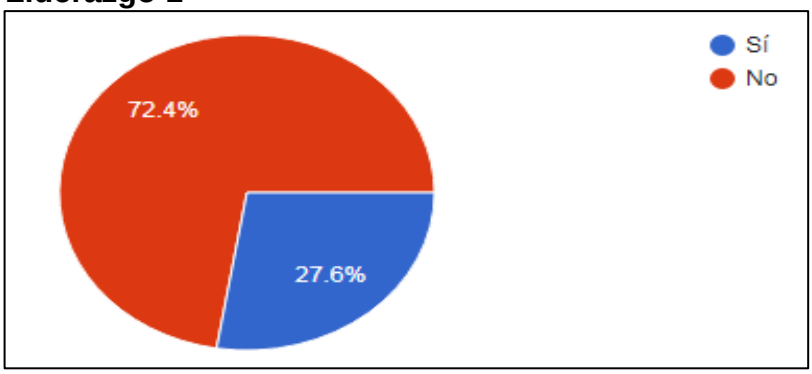


Fuente: Los autores

La gráfica 20 muestra que el 69% dice que la dirección SI provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI y el 31% dice que NO, lo anterior obedece a que los usuarios tienen la percepción de que al ser dotados con equipos tecnológicos para el ejercicio de sus labores ya cuentan con los recursos suficientes para cumplir los objetivos del Sistema de gestión de Seguridad de la Información.

• ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?

Gráfica 21. Test de Cumplimiento Norma 27001:2013. Liderazgo 1



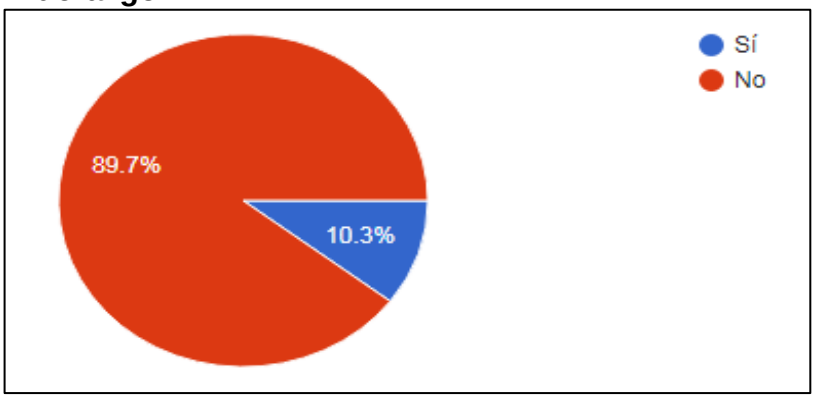
Fuente: Los autores

La gráfica 21 evidencia que el 72.4% dice que la dirección NO revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI y el 27.6% dice que SI, lo anterior obedece a que se tienden a generar confusiones entre la revisión de las actividades o funciones propias de los cargos de los funcionarios

y la revisión de los objetivos del Sistema de Gestión de Seguridad de la información.

• ¿Se ha definido una Política de la Seguridad de la Información?

Gráfica 22. Test de Cumplimiento Norma 27001:2013. Liderazgo 2

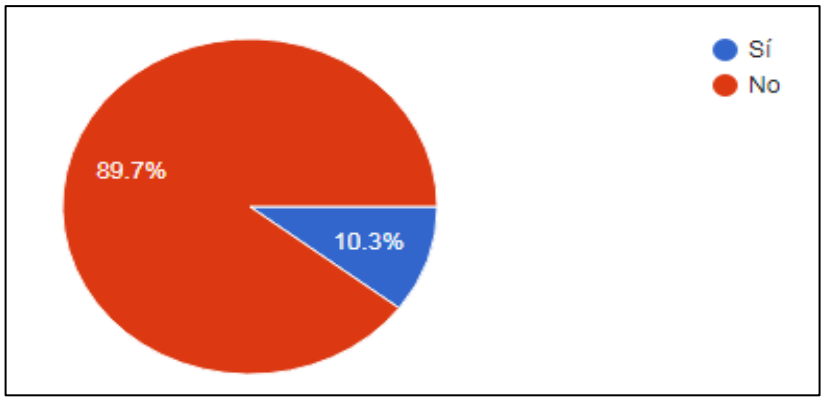


Fuente: Los autores

En la gráfica 22 se muestra que el 89.7% dice que NO se ha definido una Política de la Seguridad de la Información y el 10.3% dice que SI, lo anterior obedece a que los usuarios tienen la percepción de que al contar con usuarios de red propios y hacer uso de recursos para la protección de equipos ya existe una política de seguridad.

• ¿Conoce los riesgos y el plan de tratamiento de riesgos para la seguridad de la información?

Gráfica 23. Test de Cumplimiento Norma 27001:2013. Planificación 1



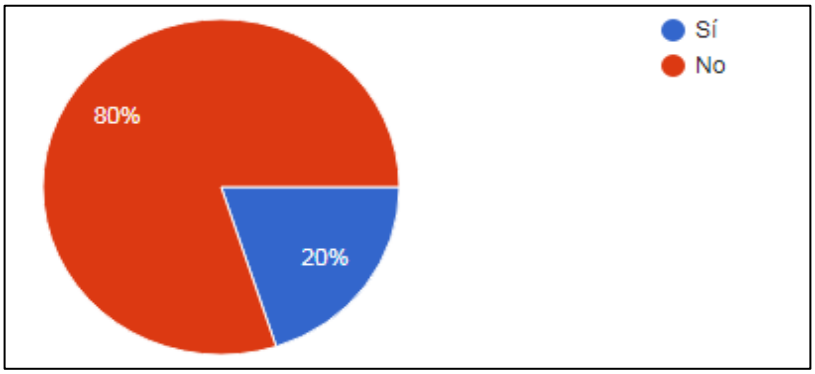
Fuente: Los autores

La gráfica 23 evidencia que el 89.7% dice que NO conoce los riesgos y el plan de tratamiento de riesgos para la seguridad de la información y el 10.3% dice que SI,

lo anterior obedece a que, aunque no se tiene definido un plan de tratamiento de riesgo para la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón, tampoco se socializa con los usuarios su definición y por ende a que riesgos están expuestos.

• ¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón teniendo en cuenta las funciones principales dentro de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón?

Gráfica 24. Test de Cumplimiento Norma 27001:2013. Planificación 2

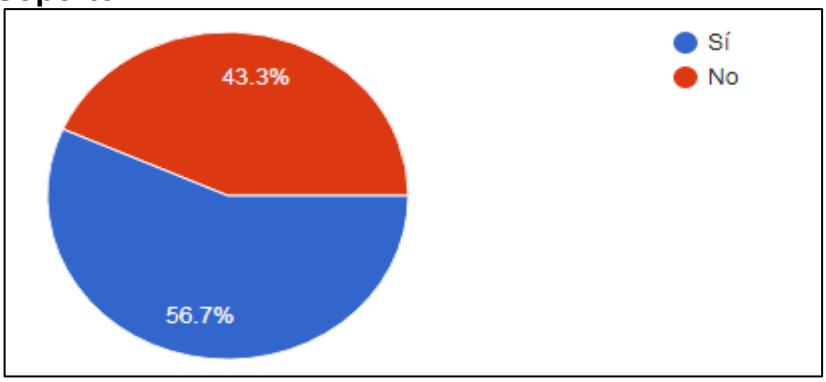


Fuente: Los autores

En la gráfica 24 se aprecia que el 80% dice que NO se han integrado los objetivos de la Seguridad de la Información en los procesos de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón y el 20% dice que SI, lo anterior se debe a que a que el 80% de los usuarios manifiesta que tiene una idea no del todo clara en relación con los objetivos del negocio los que se puede apoyar con capacitaciones de cara a los usuarios finales.

• ¿Se identifican y asignan los recursos necesarios para el SGSI?

Gráfica 25. Test de Cumplimiento Norma 27001:2013. Soporte 1

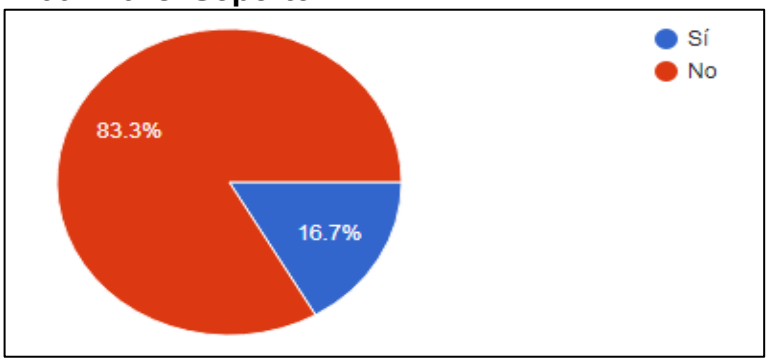


Fuente: Los autores

La gráfica 25 muestra que el 56.7% dice que SI se identifican y asignan los recursos necesarios para el SGSI y el 43.3% dice que NO, lo anterior obedece a que los usuarios en general no tienen claridad en cuales son los recursos que se deben asignar para apalancar un Sistema de Gestión de Seguridad de la Información.

• ¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?

Gráfica 26. Test de Cumplimiento Norma 27001:2013. Soporte 2

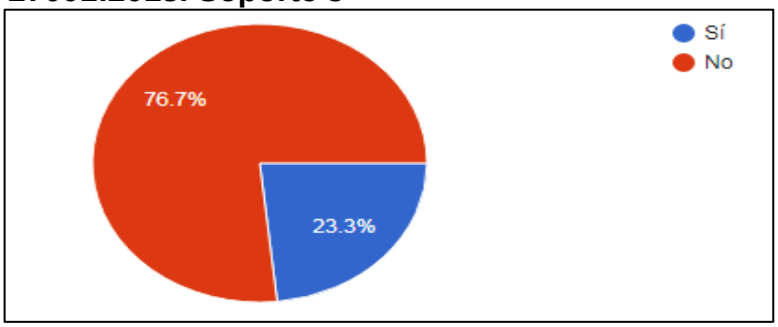


Fuente: Los autores

En la gráfica 26 es evidente que el 83.3% dice que NO se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad y el 16.7% dice SI, lo anterior evidencia que claramente la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón requiere capacitación constante a los funcionarios en relación a la seguridad de la información teniendo en cuenta que no solo se evalúan competencias si no que a su vez se genera un cambio de conciencia organizacional.

• ¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?

Gráfica 27. Test de Cumplimiento Norma 27001:2013. Soporte 3

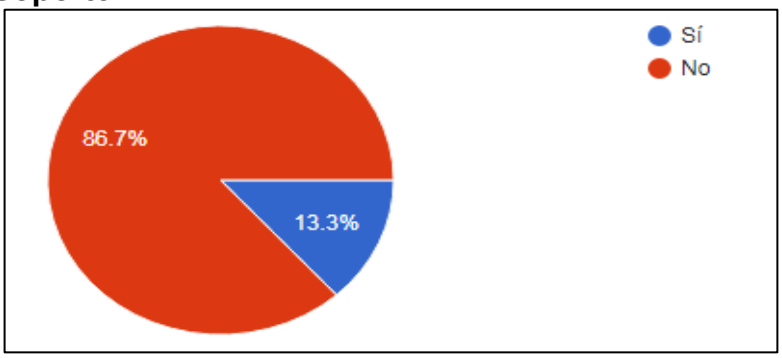


Fuente: Los autores

En la gráfica 27 se muestra que el 76.7% dice que el personal NO está involucrado y es consciente de su papel en la Seguridad de la Información y el 23.3% dice que SI, lo anterior obedece a que los usuarios no tienen del todo claro en relación con que papel desempeñan dentro del Sistema de Gestión de Seguridad de la Información.

- ¿Se comunica la política y los temas relacionados con la Seguridad de la Información con las responsabilidades de cada uno?

Gráfica 28. Test de Cumplimiento Norma 27001:2013. Soporte 4

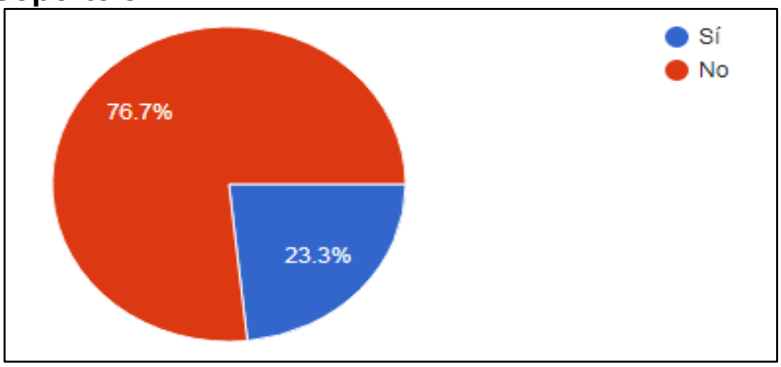


Fuente: Los autores

En la gráfica 28 se muestra que el 86.7% dice que NO se comunica la política y los temas relacionados con la Seguridad de la Información con las responsabilidades de cada uno y el 13.3% dice que SI, lo anterior obedece a que se genera confusiones entre los usuarios en relación con políticas o reglamento internos de trabajo y políticas de seguridad de la información que claramente no están definidas.

- ¿Se cuenta con procedimientos documentados para la seguridad de la información en la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón?

Gráfica 29. Test de Cumplimiento Norma 27001:2013. Soporte 5

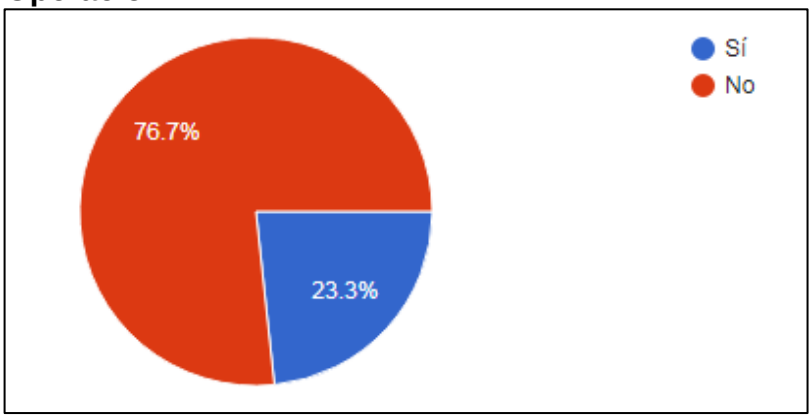


Fuente: Los autores

En la gráfica 29 se evidencia que el 76.7% dice que NO se cuenta con procedimientos documentados para la seguridad de la información en la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón y el 23.3% dice que SI, lo anterior obedece a que, aunque si tienen alguna documentación, esta no es del todo clara y socializada, lo anterior permite evidenciar que se debe buscar un afinamiento y se debe socializar a los interesados dichos documentos a fin de tener claridad con relación a la Seguridad de la información.

• ¿Conoce los riesgos y el tratamiento de estos en cuestiones de Seguridad de la Información?

Gráfica 30. Test de Cumplimiento Norma 27001:2013. Operación

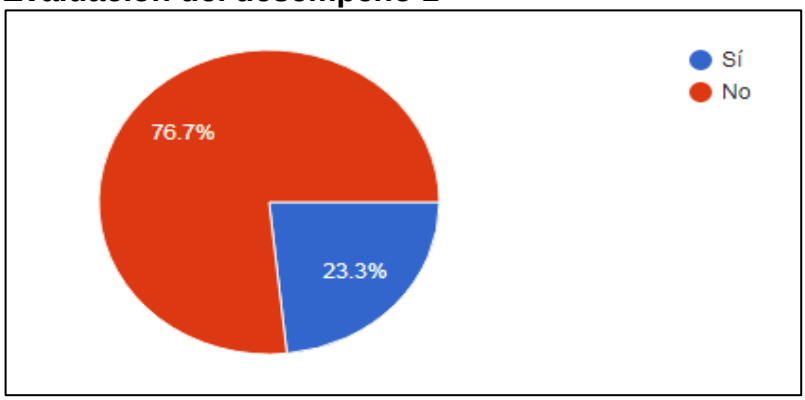


Fuente: Los autores

En la gráfica 30 se muestra que el 76.7% dice que NO conoce los riesgos y el tratamiento de estos en cuestiones de Seguridad de la información y el 23.3% dice que SI. Lo anterior evidencia que un 76.7% de los usuarios requieren capacitación en relación con los riesgos presentes durante el ejercicio de las funciones propias de los cargos y el 23.3% aunque tiene una idea se debe reforzar en temáticas de seguridad de la información para buscar un engranaje en donde se contextualice el tratamiento a seguir con los riesgos presentes.

• ¿Se hace seguimiento y medición de los riegos en la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón?

Gráfica 31. Test de Cumplimiento Norma 27001:2013. Evaluación del desempeño 1

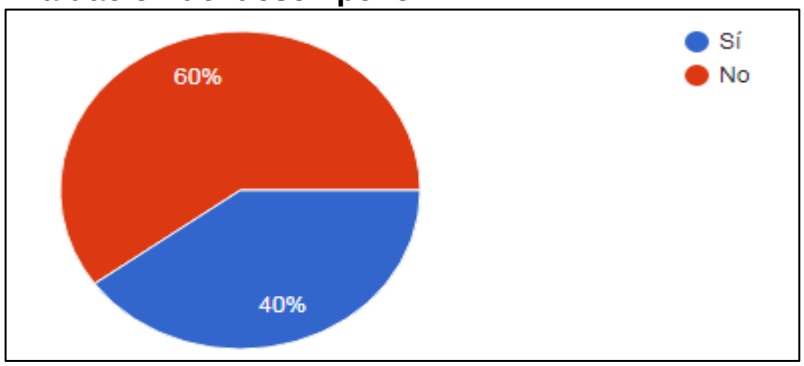


Fuente: Los autores

La gráfica 31 evidencia que el 76.7% dice que No se hace seguimiento y medición de los riegos en la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón y el 23.3% dice que SI, lo anterior obedece a que a que el 76.7% infieren en que internamente o se cuenta con el recurso humano necesario para realizar dicha actividad, por otro lado, el 23,3 % percibe que esta actividad debe recaer sobre el Dpto. de tecnología directamente.

• ¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?

Gráfica 32. Test de Cumplimiento Norma 27001:2013. Evaluación del desempeño 2

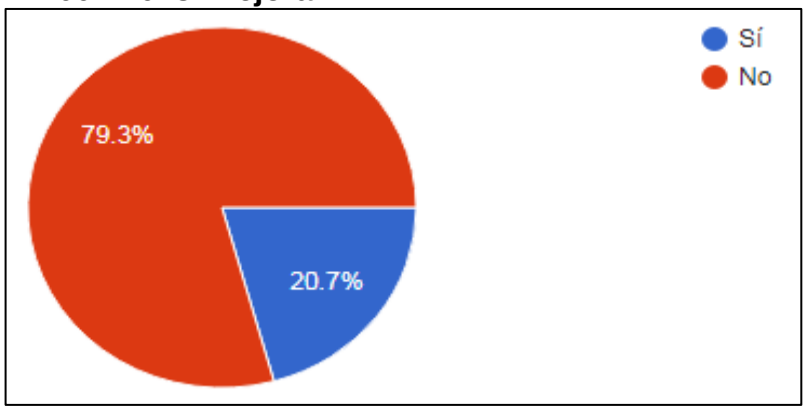


Fuente: Los autores

En la gráfica 32 es evidente que el 60% dice que NO Existe una programación para los informes de la dirección y existe constancia de su realización periódica y el 40% dice que SI, lo anterior obedece a que a que el 60% de los usuarios manifiesta no tener claridad a qué tipo de informes se hace alusión lo permite indagar que no se contextualiza a los usuarios en qué punto se encuentra la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón en temas de Seguridad de la información.

• ¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?

Gráfica 33. Test de Cumplimiento Norma 27001:2013. Mejora



Fuente: Los autores

La gráfica 33 muestra que el 79.3% dice que NO existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora y el 20.7% dice que SI, lo anterior obedece a que el 79.3% de los usuarios al tener una idea sobre la definición de un Sistema de Gestión de Seguridad de la Información consideran que se deben realizar ajustes en temas de socialización con el propósito de tener una claridad sobre su rol dentro del SGSI, el 20.7% manifestó que existe un proceso pero no se tiene claro cuál es por lo que se indaga que se debe afinar en todo tiempo la contextualización involucrando a las partes que hacen parte el SGSI

Triangulación de resultados entre los dos instrumentos aplicados. A continuación, se describen algunas reflexiones extraídas como resultado de la aplicación del cuestionario ISO/IEC 27001:2013 a la alta Gerencia y la encuesta a los funcionarios de los procesos misionales;

• La Curaduría Urbana N.3 Arq. Ana María Cadena Tobón tiene elementos de protección que proporciona cierto de grado de seguridad en infraestructura tecnológica, sin embargo, estos deben apalancados por medio de procedimientos que garanticen la seguridad de la información.

• Se debe hacer partícipe a todos los actores que hacen parte de los procesos misionales en la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón a fin de poner en contexto en relación con la seguridad de la información socializando su rol.

• Es importante apalancar la seguridad de la información por medio de capacitaciones constantes en donde se involucren proveedores y las diferentes áreas que hacen parte de los procesos misionales organizaciones.

- Al tomar como base el cuestionario ISO/IEC 27001:2013 para aplicar el instrumento a la Alta Dirección se evidencia que la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón presenta ciertos avances en relación con algunos dominios y controles de la norma ISO/IEC 27001:2013.

- La encuesta aplicada a los funcionarios permitió evidencia que hay confusiones en manejos de términos.

- Los funcionarios no tienen claridad total en relación con la definición de un Sistemas de Gestión de Seguridad de la Información, sus componentes y cómo interactúan dentro de los procesos misionales.

- No hay una clara conciencia por parte de los usuarios precisamente porque no se socializa con ellos los riesgos los que se expone los activos de información y como estos se pueden tratar.

- Al no tener definida una política de Seguridad de la Información se incurre en malas prácticas lo que genera que se vulnere la Seguridad de la información exponiendo la Integridad, Disponibilidad y confidencialidad de los activos de información.

- Se requiere de manera prioritaria la creación e implementación de políticas de Seguridad de la Información de tal modo que esta se socialicen a los usuarios para ser adoptadas en el desarrollo de las funciones propias de los cargos.

5.2 FASE DE INTERVENCIÓN

La propuesta de intervención se desarrolla teniendo en cuenta los resultados obtenidos en la subfase de diagnóstico con la aplicación del cuestionario ISO/IEC 27001:2013 a la Gerencia y la Coordinadora Administrativa y SIG, la encuesta dirigida a los funcionarios que hacen parte de los procesos misionales y la triangulación entre estos dos instrumentos.

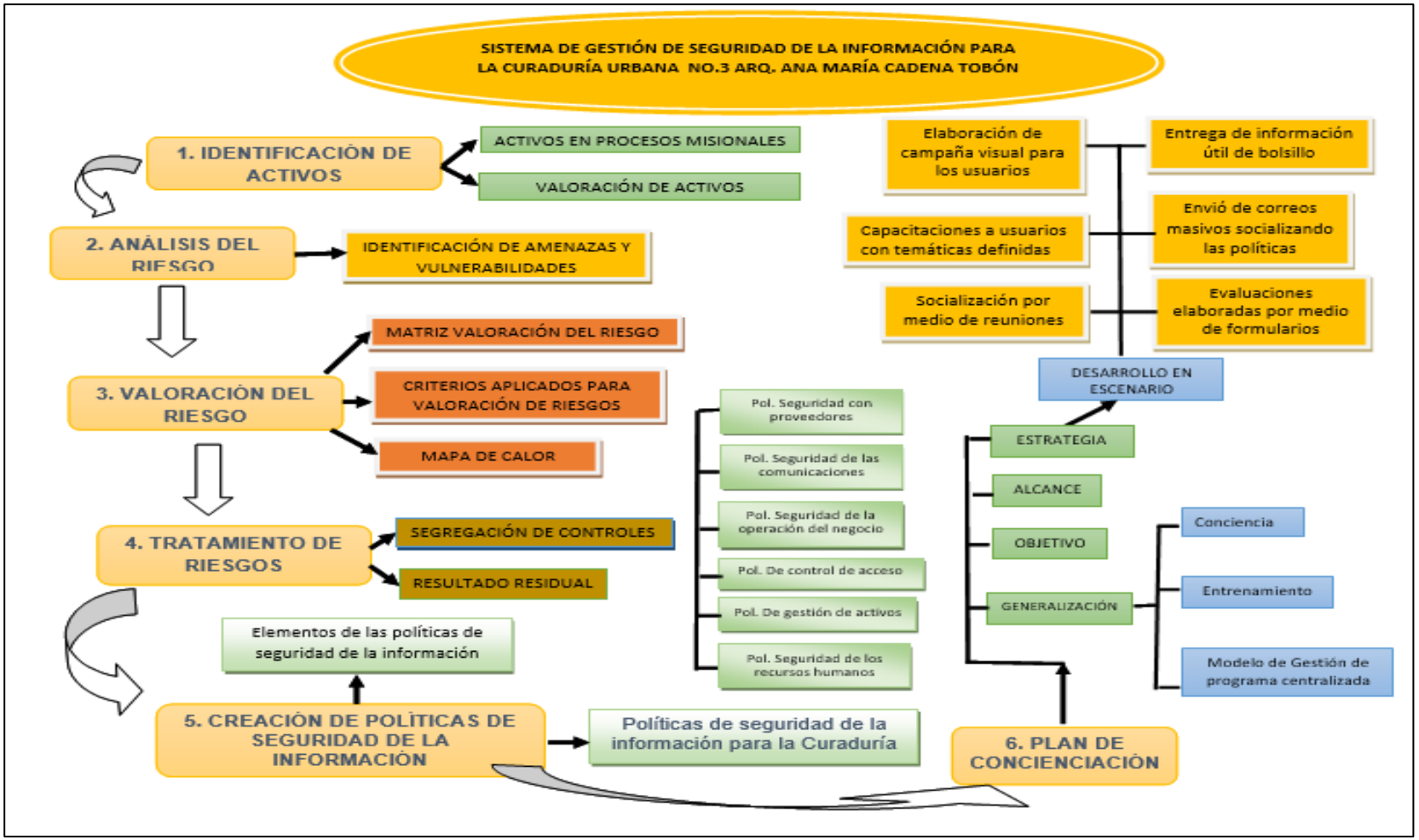
En correspondencia con lo anterior, se materializa para la Curaduría Urbana No. 3 Arq. Ana María Cadena Tobón el diseño de un Sistema de Gestión de Seguridad de la Información. Por tanto, esta fase de intervención describe una subfase dedicada a la elaboración de dicho diseño.

5.2.1 Subfase de diseño de SGSI. Para el desarrollo del Sistema de Gestión de Seguridad de la Información que requiere la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón y de acuerdo a los resultados obtenidos en la fase de exploración, se hace necesario tener en cuenta los controles que menciona la Norma ISO/IEC 27001:2013, atendiendo a la consecución de los siguientes pasos: Identificación de activos, Análisis de riesgo, Valoración del riesgo, Tratamiento del riesgo, Creación

de Políticas de seguridad de la información, plan de concienciación.

A continuación, se presenta un esquema que describe los elementos que contiene el Diseño del Sistema de Gestión de Seguridad de la Información para la Curaduría Urbana No.3 Arq. Ana María cadena Tobón ver figura 37 seguidamente se describe cada uno de los pasos que contiene el diseño.

Figura 4. Elementos del SGSI en la Curaduría Urbana No.3



Fuente: Los Autores

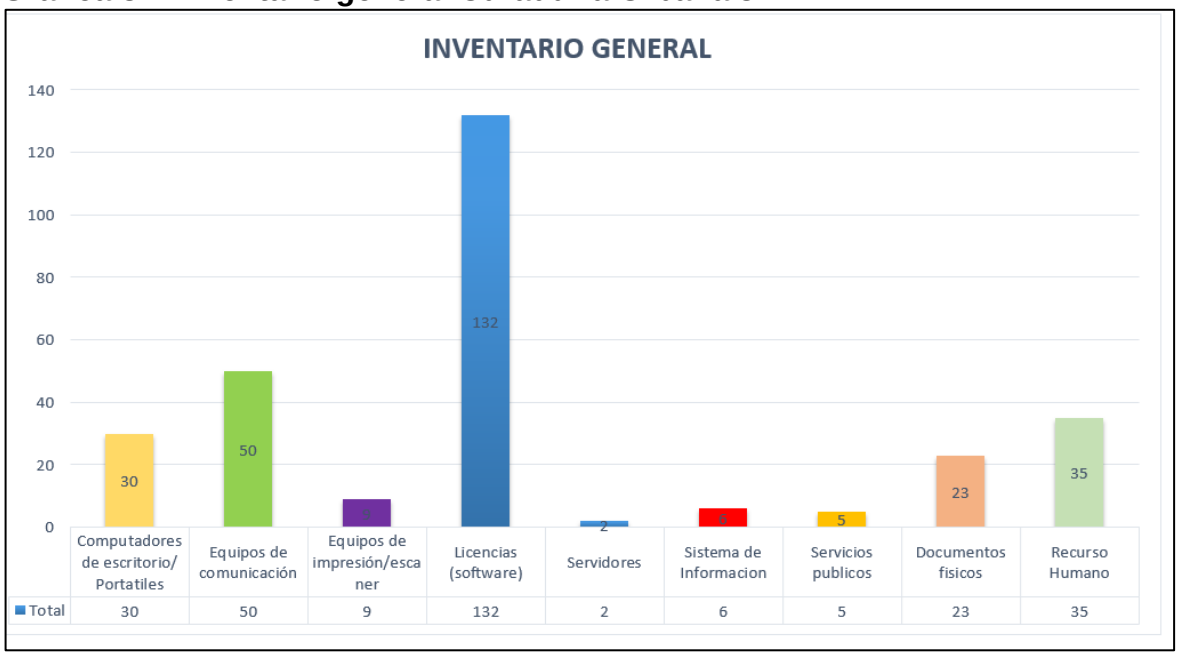
6. IDENTIFICACIÓN DE ACTIVOS

6.1 ACTIVOS EN PROCESOS MISIONALES

En visitas realizadas a las instalaciones de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, se realizó la valoración de activos que se encuentran en la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón con el propósito de realizar una clasificación de acuerdo con como la norma lo sugiere en el Anexo A.8.1.1, estos se describen a continuación en relación con los procesos misionales. (Ver grafica 34) y cuadros 3 y 4 que desglosa el inventario general de la Curaduría).

- Hardware.
- Software.
- Información.
- Servicios públicos.
- Recurso humano.

Gráfica 34. Inventario general Curaduría Urbana 3.



Fuente: Los autores

Cuadro 3. Inventario Global Curaduría Urbana No. 3 - Parte 1

Cod. Activo	Proceso	Activo	Tipo activo	Cantidad
A1	Procesos Misionales	Licencia Windows Server 2012 R2 Standar Servidor Aplicaciones	Software	2
A2	Procesos Misionales	Licencia ZW CAD	Software	17
A3	Procesos Misionales	Licencia Argis Basic for Desktop 10.5	Software	4
A4	Procesos Misionales	Visor TaktuGIS	Software	17
A5	Procesos Misionales	Licencia Windows 10 Pro OEM	Software	59
A6	Procesos Misionales	Licencia Office 2010 Home and Bussines	Software	20
A7	Procesos Misionales	Licencia Office 2013 Home and Bussines	Software	7
A8	Procesos Misionales	Licencia Office 2016 Home and Bussines	Software	3
A9	Procesos Misionales	Licencia Office 2010 Profesional	Software	2
A10	Procesos Misionales	Licencia Adobe Acrobat XI Pro	Software	1
A11	Procesos Misionales	Canal dedicado MPLS de 2 MB SDP CU3	Servicios Públicos	1
A12	Procesos Misionales	Canal de internet de 30 MB CU3	Servicios Públicos	1
A13	Procesos Misionales	Línea telefónica 1 PBX	Servicios Públicos	1
A14	Procesos Misionales	Página Web	Digital	1
A15	Expedición, Entrega y Notificación	Línea telefónica 2 Vecinos	Servicios Públicos	1
A16	Estudios Técnicos	Coordinador Construcción	Recurso Humano	2
A17	Estudios Técnicos	Coordinador Jurídica	Recurso Humano	1
A18	Estudios Técnicos	Coordinador Ingeniería	Recurso Humano	1
A19	Estudios Técnicos	Arq.uitecto de Análisis	Recurso Humano	10
A20	Estudios Técnicos	Asistente Jurídico	Recurso Humano	2
A21	Estudios Técnicos	Ingeniero Catastral	Recurso Humano	1
A22	Procesos Misionales	Administrador de Sistemas	Recurso Humano	1
A23	Procesos Misionales	Asistente Curaduría	Recurso Humano	1
A24	Emisión de Conceptos	Auxiliar Consultas, Conceptos y Zonificación	Recurso Humano	2
A26	Procesos Misionales	Director Administrativo	Recurso Humano	1
A27	Estudios Técnicos	Ingeniero de Análisis	Recurso Humano	3
A28	Expedición, Entrega y Notificación	Notificador	Recurso Humano	1
A29	Radicación	Radicador	Recurso Humano	3
A30	Estudios Técnicos	Coordinadora Urbanismo	Recurso Humano	1
A31	Estudios Técnicos	Abogado de Análisis	Recurso Humano	3
A32	Procesos Misionales	Curaduría	Recurso Humano	1
A33	Expedición, Entrega y Notificación	Licencias de construcción	Documento Físico	1
A34	Expedición, Entrega y Notificación	Licencias de intervención espacio publico	Documento Físico	1
A35	Expedición, Entrega y Notificación	Licencias de modificación de planos urbanísticos	Documento Físico	1

Cuadro 3. (Continuación)

Cod. Activo	Proceso	Activo	Tipo activo	Cantidad
A36	Expedición, Entrega y Notificación	Licencias de parcelación	Documento Físico	1
A37	Expedición, Entrega y Notificación	Licencias de subdivisión	Documento Físico	1
A38	Expedición, Entrega y Notificación	Licencias de urbanización	Documento Físico	1
A39	Expedición, Entrega y Notificación	Licencias para la construcción de piscinas	Documento Físico	1
A40	Expedición, Entrega y Notificación	Licencias para planos de alinderamiento y cuadros de áreas de propiedad horizontal	Documento Físico	1
A41	Expedición, Entrega y Notificación	Resoluciones	Documento Físico	1
A42	Procesos Misionales	Acta Reunión y/o Comité	Documento Físico	1
A44	Procesos Misionales	Informes de auditorias	Documento Físico	1
A45	Procesos Misionales	Correspondencia Enviada	Documento Físico	1
A46	Procesos Misionales	Correspondencia Recibida	Documento Físico	1
A47	Estudios Técnicos	Planilla de control movimiento expedientes puestos de trabajo	Documento Físico	1
A48	Procesos Misionales	Programa auditoría	Documento Físico	1
A49	Procesos Misionales	Solicitud de Acciones de Mejora	Documento Físico	1
A50	Estudios Técnicos	Zonificación	Documento Físico	1
A51	Estudios Técnicos	Lista de chequeo por área	Documento Físico	1
A52	Estudios Técnicos	Inventario expedientes	Documento Físico	1
A53	Procesos Misionales	Traslado de Documentos	Documento Físico	1
A54	Procesos Misionales	Control de requerimientos sistema de información	Documento Físico	1
A55	Procesos Misionales	Control de requerimientos soporte	Documento Físico	1
A56	Procesos Misionales	Backup de información almacenada en discos duros externos	Digital	1
A57	Procesos Misionales	Base de datos en access para consulta de expedientes antiguos	Digital	1
A58	Procesos Misionales	Aplicación y base de datos a la medida para el manejo de información y trazabilidad de los expedientes	Digital	1
A59	Procesos Misionales	Servidor virtual de impresión.	Digital	1
A60	Procesos Misionales	Servidor virtual glpi.	Digital	1
A61	Procesos Misionales	Sistema de Información ARC-GIS	Digital	1
A62	Procesos Misionales	SINUPOT / GEOPORTAL	Digital	1

Fuente: Los Autores

Cuadro 4. Inventario Global Curaduría Urbana No. 3 Parte 2

Cod. Activo	Proceso	Activo	Tipo activo	Cantidad	Cod. Activo
A63	Procesos Misionales	Todo en uno Lenovo E72z	Intel® Core™ i5-2400S 2.50 GHz, 120GB SSD, 4GB RAM	Hardware PC	3
A64	Procesos Misionales	Equipo de mesa HP ProDesk 600 G1 DM	Intel® Core™ i3-4160 CPU @ 3,60 GHz,120GB SSD, 8GB RAM	Hardware PC	8
A65	Procesos Misionales	Equipo de mesa ZBOX-ZBOX-MI543NANO-U	Intel® Core™ i5-6200U 2,40 GHz, 120 GB SSD, 8GB RAM	Hardware PC	10
A66	Procesos Misionales	Portátil G3	Intel® Core™ i7-8750H CPU@ 2,20 GHz (12 CPUs), 250 GB SSD, 16 GB RAM	Hardware PC	1
A67	Procesos Misionales	Todo en uno HP Compaq Pro 4300	Intel® Core™ i3-3220 3.30 GHz, 500 GB DD, 4 GB RAM	Hardware PC	2
A68	Procesos Misionales	Todo en uno HP TouchSmart Elite 7320	Intel® Core™ i5-2400S 2.50 GHz, 500 GB DD, 8 GB RAM	Hardware PC	1
A69	Procesos Misionales	Todo en uno Lenovo E73z	Intel® Core™ i3-4130 3,40 GHz, 120GB SSD, 4GB RAM	Hardware PC	2
A70	Procesos Misionales	Todo en uno Lenovo F0D1	Intel® Core™ i7-7700T (8 CPUs) 2.90 GHz, 2TB DD, 8GB RAM	Hardware PC	1
A71	Procesos Misionales	Todo en uno Lenovo M72z	Intel® Core™ i5-3470S 2.90 GHz, 500 GB DD, 4 GB RAM	Hardware PC	1
A72	Procesos Misionales	Servidor de aplicaciones HP Proliant DL380 G6	Intel® Xeon® CPU X5650 @ 2.67 GHz (2processors), 3TB DD, 38 GB RAM	Hardware Servidor	1
A73	Procesos Misionales	Servidor de aplicaciones HP Proliant DL380 G6	Intel® Xeon® CPU X5650 @ 2.67 GHz (2processors), .2.5TB, 32 GB RAM	Hardware Servidor	1
A74	Procesos Misionales	Planta telefónica AVAYA	Ip Office 500 v2	Hardware Com.	1
A75	Procesos Misionales	Teléfonos Planta AVAYA	Modelo 1608 IP	Hardware Com.	35

Cuadro 4. (Continuación)

Cod. Activo	Proceso	Activo	Tipo activo	Cantidad	Cod. Activo
A76	Procesos Misionales	Switch 48 puertos HP	HP ProCurve 2910al	Hardware Com.	1
A77	Procesos Misionales	Switch 24 puertos HP	HP ProCurve 2910al	Hardware Com.	2
A78	Procesos Misionales	Router inalámbrico telefónica	Cisco 2801	Hardware Com.	1
A75	Procesos Misionales	Teléfonos Planta AVAYA	Modelo 1608 IP	Hardware Com.	35
A76	Procesos Misionales	Switch 48 puertos HP	HP ProCurve 2910al	Hardware Com.	1
A77	Procesos Misionales	Switch 24 puertos HP	HP ProCurve 2910al	Hardware Com.	2
A78	Procesos Misionales	Router inalámbrico telefónica	Cisco 2801	Hardware Com.	1
A79	Procesos Misionales	Firewall	Fortinet	Hardware Com.	1
A80	Procesos Misionales	AP Unifi	AP AC LR	Hardware Com.	3
A81	Procesos Misionales	DVR	Dahua 32 Canales 1080p Full Hd 2 Megapixel Pentahibrido	Hardware Com.	1
A82	Procesos Misionales	UPS	CDP TRIFASICA DE 20KVA PF365	Hardware	1
A83	Procesos Misionales	Celulares	Motorola e4	Hardware	2
A84	Procesos Misionales	Impresora multifuncional	RICOH MP 501	Hardware Imp	1
A85	Procesos Misionales	Impresora multifuncional	Epson L3110	Hardware Imp	1

Fuente: Los autores

6.2 VALORACIÓN DE ACTIVOS

Una vez se realizó el inventario de activos, se elaboró una matriz de valoración de activos con el propósito de tener un panorama en relación con la responsabilidad que cada integrante que conforman los procesos misionales tiene en relación con estos activos de información en diferentes ámbitos. Se resalta que la aplicación de esta matriz visualiza los criterios a tener en cuenta en dado caso que se vulnere las cualidades de la información.

6.2.1 Atributos de seguridad. Se definieron criterios establecidos con el fin de obtener una valoración con el propósito de tener una escala que permita visualizar una medición para realizar un análisis en grado de importancia, estos criterios se describen a continuación:

- **Criterio disponibilidad**

Valoración alta (3): de acuerdo con este criterio se establece que el activo de información deberá estar siempre disponible para cualquier miembro activo de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

Valoración media (2): el activo de información no deberá estar más de 3 horas fuera de servicio.

Valoración baja (1): el activo de información no deberá estar más de 1.5 horas fuera de servicio.

- **Criterio integridad**

Valoración Alta (3): teniendo en cuenta variables como tipo de archivo, tamaño, ubicación la información se podrá restaurar en un tiempo estimado de 5 horas, tiempo en el cual se realizará las indagaciones pertinentes.

Valoración Media (2): teniendo en cuenta variables como tipo de archivo, tamaño, ubicación la información se podrá restaurar en un tiempo estimado de 4 días, tiempo en el cual se realizará las indagaciones pertinentes.

Valoración Baja (1): teniendo en cuenta variables como tipo de archivo, tamaño, ubicación la información se podrá restaurar en un tiempo estimado de 8 días, tiempo en el cual se realizará las indagaciones pertinentes.

- **Criterio confidencialidad**

Valoración Alta (3): la información física y magnética que reposa en los sistemas de información de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón se utiliza única y exclusivamente por los integrantes activos que estén justificados por

medio de contrato laboral, la información será confidencial en su totalidad.

Valoración Media (2): la información física y magnética que reposa en los sistemas de información de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón se utiliza única y exclusivamente por los integrantes activos que estén justificados por medio de contrato laboral la cual se puede utilizar es situaciones que lo requieran (auditorías internas y externas).

Valoración Baja (1): la información física y magnética que reposa en los sistemas de información de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón se utiliza única y exclusivamente por los integrantes activos que estén justificados por medio de contrato laboral para fines de tratamiento o relación directa con proveedores.

6.2.2 Ponderado general de criterios. De acuerdo con los establecido anteriormente, el ponderado general consiste en realizar la sumatoria total por cada valoración en donde a nivel general 1 equivale a la valoración mínima, 2 equivale a la valoración media y 3 a la valoración máxima. (Ver cuadro 5)

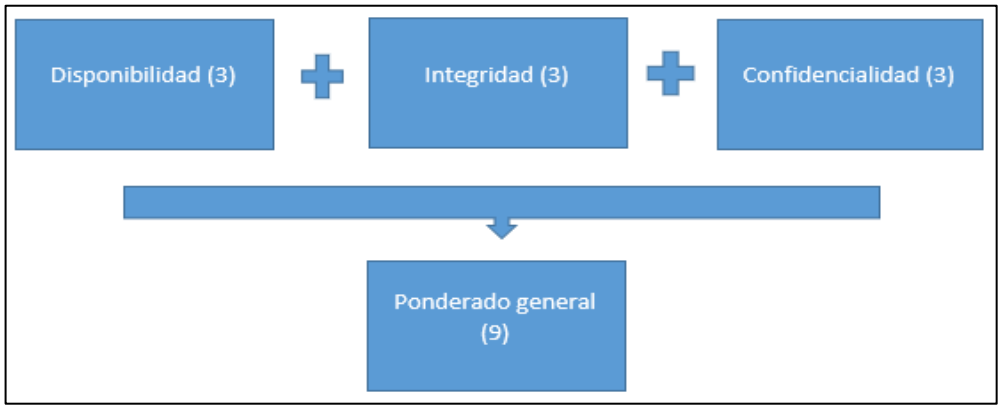
Cuadro 5. Niveles de los criterios para la valoración de los activos.

ALTO	3
MEDIO	2
BAJO	1

Fuente: Los autores

Por lo anterior se toma la máxima calificación para los criterios de Disponibilidad, integridad y confidencialidad y se realiza la sumatoria como aparece en la figura 5

Figura 5. Ponderado de los criterios para la valoración de los activos.



Fuente: Los autores

Con base en los resultados anteriores se elabora un matriz calificadora con el propósito de identificar el grado de importancia y su impacto al momento de realizar una valoración aplicada a los activos de información que conforman los procesos misionales en la Curaduría Urbana No. 3 Arq. Ana María Cadena Tobón, esta se describe en el cuadro 6.

Cuadro 6. Cualificación valoración de activos.

Importancia	Valoración
Alto	9
	8
Medio	7
	6
	5
Bajo	4
	3

Fuente: Los autores

Una vez se tienen definidos los valores por medio de la anterior escala, se procede a aplicar esta valoración a los activos que hacen parte del proceso misional en la Curaduría urbana No. 3 Arq. Ana María Cadena Tobón con el propósito de tener un panorama claro que permita continuar la aplicabilidad de un análisis de vulnerabilidades, estos activos se describen a continuación. (Ver cuadro 7).

Cuadro 7. Valoración de activos Curaduría Urbana No. 3.

No	Descripción	Tipo	Disponibilidad	Integridad	Confidencialidad	Importancia
A1	Licencia Windows Server 2012 R2 Standar Servidor Aplicaciones	Software	3	2	2	7
A2	Licencia ZW CAD	Software	3	2	2	7
A3	Licencia Argis Basic for Desktop 10.5	Software	3	2	2	7
A4	Visor TaktuGIS	Software	3	2	2	7
A5	Licencia Windows 10 Pro OEM	Software	3	2	2	7
A6	Licencia Office 2010 Home and Bussines	Software	3	2	2	7
A7	Licencia Office 2013 Home and Bussines	Software	3	2	2	7
A8	Licencia Office 2016 Home and Bussines	Software	3	2	2	7
A9	Licencia Office 2010 Profesional	Software	3	2	2	7
A10	Licencia Adobe Acrobat XI Pro	Software	3	2	2	7
A11	Canal dedicado MPLS de 2 MB SDP CU3	Servicios Públicos	3	3	3	9
A12	Canal de internet de 30 MB CU3	Servicios Públicos	3	3	2	8
A13	Línea telefónica 1 PBX	Servicios Públicos	1	2	3	6
A14	Hosting página Web	Servicios Públicos	3	2	1	6
A15	Línea telefónica 2 Vecinos	Servicios Públicos	1	2	2	6
A16	Coordinador Construcción	Recurso Humano	2	2	3	7
A17	Coordinador Jurídica	Recurso Humano	2	2	3	7
A18	Coordinador Ingeniería	Recurso Humano	2	2	3	7
A19	Arquitecto de Análisis	Recurso Humano	2	2	3	7
A20	Asistente Jurídico	Recurso Humano	2	2	3	7
A21	Ingeniero Catastral	Recurso Humano	2	2	3	7
A22	Administrador de Sistemas	Recurso Humano	2	2	3	7
A23	Asistente Curadora	Recurso Humano	2	2	3	7
A24	Auxiliar Consultas, Conceptos y Zonificación	Recurso Humano	2	2	3	7
A25	Coordinadora Administrativa y del SIG	Recurso Humano	2	2	3	7
A26	Director Administrativo	Recurso Humano	2	2	3	7
A27	Ingeniero de Análisis	Recurso Humano	3	3	3	7
A28	Notificador	Recurso Humano	2	2	3	7
A29	Radicador	Recurso Humano	2	2	3	7
A30	Coordinadora Urbanismo	Recurso Humano	2	2	3	7
A31	Abogado de Análisis	Recurso Humano	2	2	3	7
A32	Curadora	Recurso Humano	3	3	3	9

Cuadro 7. (Continuación)

No	Descripción	Tipo	Disponibilidad	Integridad	Confidencialidad	Importancia
A33	Licencias de construcción	Físico	2	2	3	7
A34	Licencias de intervención espacio publico	Físico	2	2	3	7
A35	Licencias de modificación de planos urbanísticos	Físico	2	2	3	7
A36	Licencias de parcelación	Físico	2	2	3	7
A37	Licencias de subdivisión	Físico	2	2	3	7
A38	Licencias de urbanización	Físico	2	2	3	7
A39	Licencias para la construcción de piscinas	Físico	2	2	3	7
A40	Licencias para planos de alinderamiento y cuadros de áreas de propiedad horizontal	Físico	2	2	3	7
A41	Resoluciones	Físico	2	2	3	7
A42	Acta Reunión y/o Comité	Físico	1	2	3	6
A43	Informe para entidad de control	Físico	1	2	3	6
A44	Informes de auditorias	Físico	1	2	3	6
A45	Correspondencia Enviada	Físico	1	2	3	6
A46	Correspondencia Recibida	Físico	1	2	3	6
A47	Planilla de Control Movimiento Expedientes puestos de trabajo	Físico	1	2	3	6
A48	Programa auditorías	Físico	1	2	3	6
A49	Solicitud de Acciones de Mejora	Físico	1	2	3	6
A50	Zonificación	Físico	1	2	3	6
A51	Lista de chequeo por área	Físico	1	2	3	6
A52	Inventario expedientes	Físico	1	2	3	6
A53	Traslado de Documentos	Físico	1	2	3	6
A54	Control de requerimientos sistema de información	Físico	1	2	3	6
A55	Control de requerimientos soporte	Físico	1	2	3	6
A56	Backup de información almacenada en discos duros externos	Datos	3	3	3	9
A57	Sistema de información en access para consulta de expedientes antiguos.	Datos	3	3	3	9
A58	Sistema de información web a la medida para el manejo de información y trazabilidad de los expedientes.	Datos	3	3	3	9

Cuadro 7. (Continuación)

No	Descripción	Tipo	Disponibilidad	Integridad	Confidencialidad	Importancia
A59	Servidor de impresión.	Datos	2	2	2	6
A60	Servidor de glip.	Datos	2	2	2	6
A61	Sistema de Información ARC-GIS	Datos	3	3	3	9
A62	SINUPOT / GEOPORTAL	Datos	3	3	3	9
A63	Todo en uno Lenovo E72z	Hardware	2	3	3	8
A64	Equipo de mesa HP ProDesk 600 G1 DM	Hardware	2	3	3	8
A65	Equipo de mesa ZBOX-ZBOX-MI543NANO-U	Hardware	2	3	3	8
A66	Portatil G3	Hardware	2	3	3	8
A67	Todo en uno HP Compaq Pro 4300	Hardware	2	3	3	8
A68	Todo en uno HP TouchSmart Elite 7320	Hardware	2	3	3	8
A69	Todo en uno Lenovo E73z	Hardware	2	3	3	8
A70	Todo en uno Lenovo F0D1	Hardware	2	3	3	8
A71	Todo en uno Lenovo M72z	Hardware	2	3	3	8
A72	Servidor de aplicaciones HP Proliant DL380 G6	Hardware	2	3	3	9
A73	Servidor de Internet HP Proliant DL380 G6	Hardware	2	3	3	9
A74	Planta telefónica AVAYA	Hardware	2	2	2	6
A75	Teléfonos Planta AVAYA	Hardware	2	2	2	7
A76	Switch 48 puertos HP	Hardware	3	3	3	9
A77	Switch 24 puertos HP	Hardware	3	3	3	9
A78	Router inalámbrico telefónica	Hardware	3	3	3	9
A79	Firewall	Hardware	3	3	3	9
A80	AP Unifi	Hardware	3	3	3	9
A81	DVR	Hardware	2	3	3	8
A82	UPS	Hardware	3	3	3	9
A83	Celulares	Hardware	2	2	3	7
A84	Impresora multifuncional RICOH MP 501	Hardware	1	1	1	3
A85	Impresora multifuncional Epson L3110	Hardware	1	1	1	3

Fuente: Los autores

7. ANALISIS DEL RIESGO

7.1 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

En el cuadro 8 se relaciona el resultado al momento realizar un análisis de vulnerabilidades a los activos de información pertenecientes a los procesos misionales que tiene la curaduría urbana No.3 Arq. Ana María Cadena Tobón, los ítems que conforman este cuadro se describen continuación:

Cuadro 8. Identificación de amenazas y vulnerabilidades

Amenaza	Id amenaza	Id Vulnerabilidad	Vulnerabilidad	Dimensiones
Daños por agua o fuego	AM1	AM1-V1	Sensibilidad del equipo a la humedad, temperatura o contaminantes.	Disponibilidad
		AM1-V2	Ubicación vulnerable a inundación	
Desastres naturales	AM2	AM2-V1	Mala segregación de las instalaciones operativas y de prueba	Disponibilidad
Corte del suministro eléctrico	AM3	AM3-V1	Afectación de servicios de energía y comunicaciones	Disponibilidad
Condiciones inadecuadas de temperatura o humedad	AM4	AM4-V1	Sensibilidad del equipo a la humedad, temperatura o contaminantes.	Disponibilidad
Errores de los usuarios	AM5	AM5-V1	Interfaz de usuario complicada.	Disponibilidad
		AM5-V2	Falta de formación y conciencia sobre seguridad.	
Fallo de servicios de comunicaciones	AM6	AM6-V1	Inadecuada seguridad del cableado.	Integridad, confidencialidad y disponibilidad
Errores del administrador	AM7	AM7-V1	Inadecuada gestión de red.	Integridad, confidencialidad y disponibilidad
Errores de configuración	AM8	AM8-V1	Configuraciones en dispositivos por defecto.	Integridad
Difusión de software dañino	AM9	AM9-V9	Conexiones a red pública desprotegidas.	Integridad, Confidencialidad, y disponibilidad
Escapes de información	AM10	AM10-V1	Uso incontrolado de sistemas de información.	Confidencialidad
Alteración accidental de la información	AM11	AM11-V1	Los derechos del usuario no se revisan regularmente.	Integridad
		AM11-V2	Copia no controlada de datos	
Destrucción de información	AM12	AM12-V1	Reemplazo inadecuado de equipos viejos	Disponibilidad
Fugas de información	AM13	AM13-V1	Desprotección en equipos móviles	Confidencialidad
Vulnerabilidad de los programas	AM14	AM14-V1	Software no documentado.	Integridad, Disponibilidad, Confidencialidad
		AM14-V2	No validación de los datos procesado.	
Errores de mantenimiento / actualización de programas (software, hardware)	AM15	AM15-V1	Software no documentado.	Integridad, Disponibilidad
		AM15-V2	Inadecuada gestión de capacidad del sistema.	
		AM15-V3	Mantenimiento inadecuado.	

Cuadro 8. (Continuación)

Amenaza	Id amenaza	Id Vulnerabilidad	Vulnerabilidad	Dimensiones
Caída de sistema por agotamiento de recurso	AM16	AM16-V1	Inadecuada gestión de capacidad del sistema.	Disponibilidad
		AM16-V2	Inadecuada gestión de red.	
		AM16-V3	Uso incontrolado de sistemas de información.	
Perdida de equipos	AM17	AM17-V1	Ausencia de sistemas de identificación y autenticación.	Disponibilidad, confidencialidad
		AM17-V2	Desprotección física de equipos.	
Indisponibilidad del personal	AM18	AM18-V1	Empleados desmotivados	Disponibilidad
		AM18-V2	Inadecuada segregación de funciones	
Manipulación de la configuración	AM19	AM19-V1	Inadecuada gestión y protección de contraseñas.	Integridad, confidencialidad, y disponibilidad
		AM19-V2	Inadecuada gestión de red.	
Abuso de privilegios de acceso	AM20	AM20-V1	Descarga no controlada internet.	Integridad, confidencialidad, y disponibilidad
		AM20-V2	Inadecuada gestión y protección de contraseñas.	
Uso no previsto	AM21	AM21-V1	Utilización de los activos de información para fines personales	Integridad, confidencialidad, y disponibilidad
Difusión de software dañino	AM22	AM22-V2	Desprotección en equipos.	Integridad, confidencialidad, y disponibilidad
Acceso no autorizado	AM23	AM23-V1	Contraseñas predeterminadas no modificadas.	Integridad, confidencialidad
Modificación deliberada de la información	AM24	AM24-V1	No validación de los datos procesados.	Integridad
Divulgación de información	AM25	AM25-V1	Falta de política que permite asegurar la no divulgación de información organizacional	Confidencialidad
Manipulación de programas	AM26	AM26-V1	Alteración intencionada de la configuración de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	Integridad, confidencialidad, y disponibilidad
Manipulación de equipos	AM27	AM27-V1	Alteración intencionada del hardware que compones los sistemas de información	Confidencialidad, disponibilidad
Denegación de servicio	AM28	AM28-V1	Carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada	Disponibilidad
Robo	AM29	AM-29-V1	Respaldo inapropiado o irregular.	Confidencialidad, disponibilidad
		AM29-V2	Protección física no apropiada.	
Virus	AM30	AM30-v1	Instalación de software no autorizado	Integridad, confidencialidad, y disponibilidad

Fuente: Los autores

Por lo anterior se identificaron las siguientes convenciones:

- **AMENAZA:** corresponde a la descripción de la amenaza.
- **ID AMENAZA:** corresponde al identificador de la amenaza.
- **ID VULNERABILIDAD:** corresponde a amenaza con la vulnerabilidad.
- **VULNERAVILIDAD:** corresponde a la descripción de la vulnerabilidad.
- **DIMENSIONES:** corresponde a la cualidad de la información afectada.

8. VALORACIÓN DEL RIESGO

Teniendo en cuenta que "la valoración del riesgo es el proceso total de identificación del riesgo, análisis del riesgo y evaluación del riesgo. se realiza el análisis pertinente se procede a realizar la valoración aplicada con base en la norma NTC-ISO 31001 para de este modo definir la probabilidad contra impacto y así tener un panorama más claro con relación a la escala de criticidad en la que se pueden ver comprometidos los activos de información que componen los procesos misionales de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón. (Ver cuadros 9 y 10).

Cuadro 9. Probabilidades valoración del riesgo

Probabilidades			
Valores	1	2	3
Criterio	Baja	Media	Alta
Frecuencia	El incidente se puede presentar una vez al año.	El incidente se puede presentar dos veces al año.	El incidente se puede presentar varias veces a la semana.
Descripción	Casi nunca se presenta incidente sobre el activo de información.	En ocasiones se presentan incidentes reportados sobre el activo de información.	Es constante el reporte de incidentes sobre el activo de información.

Fuente: Los autores

Cuadro 10. Impacto valoración del riesgo

Impacto			
Valores	1	2	3
Criterio	Baja	Media	Alta
Descripción	El incidente no afecta los objetivos estratégicos del negocio, pero afecta el activo de información.	El incidente afecta el activo de información generando contratiempos en la entrega del producto.	El incidente ocasiona colapso en los objetivos estratégicos del negocio.

Fuente: Los autores

8.1 MATRIZ VALORACIÓN DEL RIESGO

Una vez ya se tienen definidos los valores con relación a la probabilidad contra el impacto, se procede a elaborar la matriz de valoración de riesgos con el propósito de identificar cuáles son los riesgos más inherentes que se tienen dentro de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, esta matriz se define como un instrumento de medición que permite tener un panorama objetivo a la hora de realizar dicha valoración como se muestra en el cuadro 11.

Cuadro 11. Probabilidad por impacto valoración del riesgo

Impacto				PROBABILIDAD
Criterio	Bajo 1	Medio 2	Alto 3	
Bajo 1	**1**	**2**	**3**	
Medio 2	**2**	**4**	**6**	
Alto 3	**3**	**6**	**9**	

Fuente: Los autores

Con los valores establecidos se procede a realizar la multiplicación de probabilidad por impacto dando como resultado el riesgo, una vez se tiene este valor se continúa realizando una tipificación con el propósito de establecer que riesgos son bajos y cuales se consideran más altos, esta descripción se menciona a continuación:

8.2 CRITERIOS APLICADOS PARA VALORACIÓN DE RIESGOS

8.2.1 Riesgo bajo valor 1-2. No se considera un riesgo suficientemente significativo dado que el objetivo estratégico de negocio no tendría un impacto mayor y el Core de negocio podría seguir funcionando si se presenta un incidente de seguridad menor, **para este criterio el riesgo se asume.**

8.2.2 Riesgo medio valor 3-4. En este nivel de valoración se tiene una aceptación del riesgo definida, el propósito de esta valoración va dirigido a realizar una monitorización y auditoria constante a los incidentes de seguridad reportados para evitar una trascendencia futura **para este criterio el riesgo se comparte**.

8.2.3 Riesgo alto valor 5-6. Este nivel de valoración exige una reacción oportuna a un incidente de seguridad reportado dado a que los riesgos tienen una incidencia en los objetivos estratégicos al Core de negocio, **para este criterio el riesgo se reduce**.

8.2.4 Riesgo critico 7-9. Este nivel de valoración exige la transferencia o eliminación completa de la amenaza o incidente reportado porque genera una afectación total a los objetivos estratégicos y Core de negocio, este riesgo exige que su nivel de atención sea prioritario a fin de tener una continuidad en las operaciones. **Para este criterio el riesgo se evita y se trata.**

8.2.5 Aceptación de los riesgos. Luego de realizar en común acuerdo con Dirección Administrativa, el Dpto. de Calidad y los líderes de área que conforman los procesos misionales en la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, se estableció un criterio de aceptación del riesgo en donde este debe mantener un indiciador por debajo de 4 correspondiente a riesgo bajo y riesgo medio

obteniendo así el riesgo residual. (Ver cuadro 12)

Cuadro 12. Valoración de riesgo activo de información

ID Riesgo	ID Activo	ID Amenaza	Probabilidad	Impacto	Riesgo inherente	Grado de aceptación
R1	A1	AM21-V1	2	2	4	Se transfiere
		AM19-V1	2	2	4	Se transfiere
R2	A2	AM21-V1	2	1	2	Se asume
		AM19-V1	2	2	4	Se reduce
R3	A3	AM21-V1	2	1	2	Se asume
		AM19-V1	2	2	4	Se transfiere
R4	A4	AM21-V1	2	2	4	Se transfiere
		AM19-V1	2	2	4	Se transfiere
R5	A5	AM21-V1	2	1	2	Se asume
		AM19-V1	2	1	2	Se asume
R6	A6	AM21-V1	2	1	2	Se asume
		AM19-V1	2	1	2	Se asume
R7	A7	AM21-V1	2	1	2	Se asume
		AM19-V1	2	1	2	Se asume
R8	A8	AM21-V1	2	1	2	Se asume
		AM19-V1	2	1	2	Se reduce
R9	A9	AM21-V1	2	1	2	Se asume
		AM19-V1	2	1	2	Se asume
R10	A10	AM21-V1	2	1	2	Se asume
		AM19-V1	2	2	4	Se transfiere
R11	A11	AM6-V1	1	2	2	Se asume
		AM28-V1	1	2	2	Se asume
R12	A12	AM6-V1	1	3	3	Se transfiere
		AM28-V1	1	3	3	Se transfiere
R13	A13	AM6-V1	1	3	3	Se transfiere
		AM28-V1	1	3	3	Se transfiere
R14	A14	AM28-V1	2	2	4	Se transfiere
		AM16-V2	2	2	4	Se transfiere
R15	A15	AM6-V1	2	2	4	Se transfiere
		AM28-V1	1	2	2	Se asume
R16	A16	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R17	A17	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R18	A18	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R19	A19	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R20	A21	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R22	A22	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata

Cuadro 12. (Continuación)

ID Riesgo	ID Activo	ID Amenaza	Probabilidad	Impacto	Riesgo inherente	Grado de aceptación
R23	A23	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R24	A24	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R25	A25	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R26	A26	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R27	A27	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R28	A28	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R29	A29	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R30	A30	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R31	A31	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R32	A32	AM18-V1	2	2	4	Se transfiere
		AM18-V2	2	2	4	Se transfiere
		AM5-V2	3	3	9	Se trata
R33	A33	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R34	A34	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R35	A35	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R36	A36	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R37	A37	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R38	A38	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R39	A39	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R40	A40	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R41	A41	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R42	A42	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R43	A43	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R44	A44	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere

Cuadro 12. (Continuación)

ID Riesgo	ID Activo	ID Amenaza	Probabilidad	Impacto	Riesgo inherente	Grado de aceptación
R45	A45	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R46	A46	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R47	A47	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R48	A48	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R49	A49	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R50	A50	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R51	A51	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R52	A52	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R53	A53	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R54	A54	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R55	A55	AM1-V2	1	3	3	Se transfiere
		AM29-V1	1	3	3	Se transfiere
R56	A56	AM24-V1	2	3	6	Se reduce
		AM10-V1	2	3	6	Se reduce
		AM17-V2	2	3	6	Se reduce
		AM11-V2	2	3	6	Se reduce
		AM-29-V1	2	3	6	Se reduce
R57	A57	AM14-V2	3	3	9	Se trata
		AM5-V1	2	2	4	Se transfiere
		AM5-V2	2	3	6	Se reduce
		AM11-V1	2	3	6	Se reduce
		AM15-V1	2	1	2	Se asume
		AM15-V3	2	3	6	Se reduce
		AM20-V2	1	3	3	Se transfiere
R58	A58	AM15-V3	2	3	6	Se reduce
		AM28-V1	2	3	6	Se reduce
		AM23-V1	1	3	3	Se transfiere
		AM16-V2	1	3	3	Se transfiere
R59	A59	AM16-V1	2	2	4	Se transfiere
		AM28-V1	2	2	4	Se transfiere
R60	A60	AM16-V1	2	2	4	Se transfiere
		AM28-V1	2	2	4	Se transfiere
R61	A61	AM6-V1	1	2	2	Se asume
		AM7-V1	2	2	4	Se transfiere
		AM15-V3	2	3	6	Se reduce
		AM16-V1	2	3	6	Se reduce
R62	A62	AM16-V1	2	2	4	Se transfiere
		AM15-V3	2	2	4	Se transfiere
		AM28-V1	2	2	4	Se transfiere
R63	A63	AM1-V1	2	2	4	Se transfiere
		AM3-V1	2	3	6	Se reduce
		AM5-V2	3	3	9	Se trata
		AM15-V3	2	3	6	Se reduce

Cuadro 12. (Continuación)

ID Riesgo	ID Activo	ID Amenaza	Probabilidad	Impacto	Riesgo inherente	Grado de aceptación
		AM17-V2	2	3	6	Se reduce
		AM21-V1	2	2	4	Se transfiere
		AM30-V1	2	3	6	Se reduce
R64	A64	AM1-V1	2	2	4	Se transfiere
		AM3-V1	2	3	6	Se reduce
		AM5-V2	3	3	9	Se trata
		AM15-V3	2	3	6	Se reduce
		AM17-V2	2	3	6	Se reduce
		AM21-V1	2	2	4	Se transfiere
R65	A65	AM1-V1	2	2	4	Se transfiere
		AM3-V1	2	3	6	Se reduce
		AM5-V2	3	3	9	Se trata
		AM15-V3	2	3	6	Se reduce
		AM17-V2	2	3	6	Se reduce
		AM21-V1	2	2	4	Se transfiere
		AM30-V1	2	3	6	Se reduce
R66	A66	AM1-V1	2	2	4	Se transfiere
		AM3-V1	2	3	6	Se reduce
		AM5-V2	3	3	9	Se trata
		AM15-V3	2	3	6	Se reduce
		AM17-V2	2	3	6	Se reduce
		AM21-V1	2	2	4	Se transfiere
		AM30-V1	2	3	6	Se reduce
R67	A67	AM1-V1	2	2	4	Se transfiere
		AM3-V1	2	3	6	Se reduce
		AM5-V2	3	3	9	Se trata
		AM15-V3	2	3	6	Se reduce
		AM17-V2	2	3	6	Se reduce
		AM21-V1	2	2	4	Se transfiere
		AM30-V1	2	3	6	Se reduce
R68	A68	AM1-V1	2	2	4	Se transfiere
		AM3-V1	2	3	6	Se reduce
		AM5-V2	3	3	9	Se trata
		AM15-V3	2	3	6	Se reduce
		AM17-V2	2	3	6	Se reduce
		AM21-V1	2	2	4	Se transfiere
		AM30-v1	2	3	6	Se reduce
R69	A69	AM1-V1	2	2	4	Se transfiere
		AM3-V1	2	3	6	Se reduce
		AM5-V2	3	3	9	Se trata
		AM15-V3	2	3	6	Se reduce
		AM17-V2	2	3	6	Se reduce
		AM21-V1	2	2	4	Se transfiere
		AM30-v1	2	3	6	Se reduce
R70	A70	AM1-V1	2	2	4	Se transfiere
		AM3-V1	2	3	6	Se reduce
		AM5-V2	3	3	9	Se trata
		AM15-V3	2	3	6	Se reduce
		AM17-V2	2	3	6	Se reduce
		AM21-V1	2	2	4	Se transfiere
		AM30-V1	2	3	6	Se reduce
R71	A71	AM1-V1	2	2	4	Se transfiere
		AM3-V1	2	3	6	Se reduce

Cuadro 12. (Continuación)

ID Riesgo	ID Activo	ID Amenaza	Probabilidad	Impacto	Riesgo inherente	Grado de aceptación
		AM5-V2	3	3	9	Se trata
		AM15-V3	2	3	6	Se reduce
		AM17-V2	2	3	6	Se reduce
		AM21-V1	2	2	4	Se transfiere
		AM30-v1	2	3	6	Se reduce
R72	A72	AM1-V1	2	3	6	Se reduce
		AM1-V2	1	3	3	Se transfiere
		AM2-V1	1	3	3	Se transfiere
		AM4-V1	2	3	6	Se reduce
		AM6-V1	1	3	3	Se transfiere
		AM7-V1	1	3	3	Se transfiere
		AM15-V3	2	3	6	Se reduce
R73	A73	AM1-V1	2	3	6	Se reduce
		AM1-V2	1	3	3	Se transfiere
		AM2-V1	1	3	3	Se transfiere
		AM4-V1	2	3	6	Se reduce
		AM6-V1	1	3	3	Se transfiere
		AM7-V1	1	3	3	Se transfiere
		AM15-V3	2	3	6	Se reduce
R74	A74	AM6-V1	1	2	2	Se asume
		AM7-V1	1	2	2	Se asume
		AM15-V3	2	2	4	Se transfiere
R75	A75	AM6-V1	1	2	2	Se asume
		AM7-V1	1	2	2	Se asume
		AM15-V3	2	2	4	Se transfiere
R76	A76	AM1-V1	2	3	6	Se reduce
		AM15-V3	2	3	6	Se reduce
		AM6-V1	1	3	3	Se transfiere
R77	A77	AM1-V1	2	3	6	Se reduce
		AM15-V3	2	3	6	Se reduce
		AM6-V1	1	3	3	Se comparte
R78	A78	AM1-V1	2	3	6	Se reduce
		AM15-V3	2	3	6	Se reduce
		AM8-V1	2	3	6	Se reduce
R79	A79	AM1-V1	2	3	6	Se reduce
		AM15-V3	2	3	6	Se reduce
		AM8-V1	2	3	6	Se reduce
R80	A80	AM1-V1	2	3	6	Se reduce
		AM15-V3	2	3	6	Se reduce
		AM8-V1	2	3	6	Se reduce
R81	A81	AM1-V1	2	3	6	Se reduce
		AM15-V3	2	3	6	Se reduce
		AM8-V1	2	3	6	Se reduce
R82	A82	AM15-V3	2	2	4	Se comparte
R83	A83	AM29-V2	2	1	2	Se asume
		AM21-21	2	2	4	Se comparte
R84	A84	AM21-V2	2	2	4	Se comparte
		AM6-V1	2	2	4	Se comparte
		AM15-V3	2	2	4	Se comparte
R85	A85	AM21-V2	2	2	4	Se comparte
		AM6-V1	2	2	4	Se comparte
		AM15-V3	2	2	4	Se comparte

8.3 MAPA DE CALOR

Teniendo en cuenta que el mapa de calor es un instrumento que permite identificar cuales los activos de información que representan o tienen un alto riesgo de contraer un evento o incidente de seguridad, se hace uso de esta herramienta una vez se tiene se tiene la valoración de riesgo a los activos de información que conforman el proceso misional en la curaduría urbana No.3 Arq. Ana María Cadena Tobón, la nomenclatura utilizada se explica a continuación:

- R= equivale al identificador del riesgo.
- A= equivale al identificador del activo.
- AM = equivale a la amenaza.
- V= equivale a la vulnerabilidad.

Por lo anterior se tiene que: R1 Equivale al identificador riesgo 1, A1 equivale al identificador del activo 1, AM1 equivale a la amenaza1 y V1 equivale a la vulnerabilidad 1. Ejemplo: R1-A1-AM1-V1.

De tal modo se aplica dicha nomenclatura a los activos de información ubicándolos de modo que se obtiene la relación que aparece en el cuadro 13.

Cuadro 13. Mapa de calor

		NIVEL DE IMPACTO		
		1 Bajo	2 Medio	3 Alto
NIVEL DE PROBABILIDAD	1 Bajo		R11-A11-AM6-V1, R11-A11-AM28-V1, R15-A15-AM28-V, R74-A74-AM6-V1, R74-A74-AM7-V1, R75-A75-AM6-V1, R75-A75-AM7-V1	R12-A11-AM6-V1, R12-A11-AM28-V1, R13-A11-AM6-V1, R13-A11-AM28-V1, R33-A33-AM1-V2, R33-A33-AM29-V1, R34-A34-AM1-V2, R34-A34-AM29-V1 R35-A35-AM1-V2, R35-A35-AM29-V1, R36-A36-AM1-V2, R36-A36-AM29-V1 R37-A37-AM1-V2, R37-A37-AM29-V1, R38-A38-AM1-V2, R38-A38-AM29-V1 R39-A39-AM1-V2, R39-A39-AM29-V1, R40-A40-AM1-V2, R40-A40-AM29-V1 R41-A41-AM1-V2, R41-A41-AM29-V1,R42-A42-AM1-V2, R42-A42-AM29-V1 R43-A43-AM1-V2, R43-A43-AM29-V1, R44-A44-AM1-V2, R44-A44-AM29-V1 R45-A45-AM1-V2, R45-A45-AM29-V1, R46-A46-AM1-V2, R46-A46-AM29-V1 R47-A47-AM1-V2, R47-A47-AM29-V1, R48-A48-AM1-V2, R48-A48-AM29-V1 R49-A49-AM1-V2, R49-A49-AM29-V1, R50-A50-AM1-V2, R50-A50-AM29-V1 R51-A51-AM1-V2, R51-A51-AM29-V1, R52-A52-AM1-V2, R52-A52-AM29-V1, R58-A58-AM23-V1,R58-A58-AM16-V2, R72-A72-AM1-V2,R72-A72-AM2-V1, R72-A72-AM6-V1,R72-A72-AM7-V1, R73-A73-AM1-V2,R73-A73-AM2-V1, R73-A73-AM6-V1,R73-A73-AM7-V1, R76-A76-AM6-V1, R77-A77-AM6-V1
	2 Medio	R2-A2-AM21-V1, R3-A3-AM21-V, R5-A5-AM21-V1, R5-A5-AM19-V1, R6-A6-AM21-V1, R6-A6-AM19-V1, R7-A7-AM21-V1, R7-A7-AM19-V1, R8-A8-AM21-V1, R8-A8-AM19-V1, R9-A9-AM21-V1, R9-A9-AM19-V1, R10-A10-AM21-V1, R57-A57-AM15-V1, R61-A61-AM6-V1, R83-A83-AM29-V2	R1-A1-AM21-V1, R1-A1-AM19-V1, R2-A2-AM19-V1, R3-A3-AM19-V1, R4-A4-AM21-V1, R4-A4-AM19-V1, R10-A10-AM19-V1, R14-A14-AM28-V1, R14-A14-AM16-V2, R15-A15-AM6-V1, R16-A16-AM18-V1, R16-A16-AM18-V2, R17-A17-AM18-V1, R17-A17-AM18-V2, R18-A18-AM18-V1, R18-A18-AM18-V2, R19-A19-AM18-V1, R19-A19-AM18-V2, R20-A20-AM18-V1, R20-A20-AM18-V2, R21-A21-AM18-V1, R21-A21-AM18-V2, R22-A22-AM18-V1, R22-A22-AM18-V2, R23-A23-AM18-V1, R23-A23-AM18-V2, R24-A24-AM18-V1, R24-A16-AM18-V2, R25-A25-AM18-V1, R25-A25-AM18-V2, R26-A26-AM18-V1, R26-A26-AM18-V2, R27-A27-AM18-V1, R27-A27-AM18-V2, R28-A28-AM18-V1, R28-A28-AM18-V2, R29-A29-AM18-V1, R29-A29-AM18-V2, R30-A30-AM18-V1, R30-A30-AM18-V2, R31-A31-AM18-V1, R31-A31-AM18-V2,R32-A32-AM18-V1, R32-A32-AM18-V2, R57-A57-AM5-V1, R57-A57-AM20-V2, R59-A59-AM16-V1, R60-A60-AM16-V1, R60-A60-AM28-V1, R61-A61-AM7-V1, R62-A62-AM16-V1, R62-A62-AM15-V3, R62-A62-AM28-V1, R63-A63-AM1-V1, R63-A63-AM21-V1, R64-A64-AM1-V1, R64-A64-AM21-V1, R65-A65-AM1-V1, R65-A65-AM21-V1, R66-A66-AM1-V1, R66-A66-AM21-V1, R67-A67-AM1-V1, R67-A67-AM21-V1, R68-A68-AM1-V1, R68-A68-AM21-V1, R69-A69-AM1-V1,R69-A69-AM21-V1, R70-A70-AM1-V1, R70-A70-AM21-V1, R71-A71-AM1-V1, R71-A71-AM21-V1, R74-A74-AM15-V3, R75-A75-AM15-V3, R82-A82-AM15-V3, R83-A83-AM21-21, R84-A84-AM21-V2, R84-A84-AM6-V1, R84-A84-AM15-V3, R85-A85-AM21-V2, R85-A85-AM6-V1, R85-A85-AM15-V3	R56-A56-AM24-V1, R56-A56-AM10-V1, R56-A56-AM17-V2, R56-A45-AM11-V2, R56-A56-AM-29-V1, R57-A57-AM5-V2, R57-A57-AM11-V1, R57-A57-AM15-V3, R58-A58-AM15-V3, R58-A58-AM28-V1, R61,A61-AM15-V3, R61-A61-AM16-V1, R63-A63-AM3-V1, R63-A63-AM15-V3, R63-A63-AM17-V2, R63-A63-AM30-v1, R64-A64-AM3-V1, R64-A64-AM15-V3, R64-A64-AM17-V2, R64-A64-AM30-v1, R65-A65-AM3-V1, R65-A65-AM15-V3, R65-A65-AM17-V2, R65-A65-AM30-v1, R66-A66-AM3-V1, R66-A66-AM15-V3, R66-A66-AM17-V2, R66-A66-AM30-v1, R67-A67-AM3-V1, R67-A67-AM15-V3, R67-A67-AM17-V2, R67-A67-AM30-v1, R68-A68-AM3-V1, R68-A68-AM15-V3, R68-A68-AM17-V2, R68-A68-AM30-v1, R69-A69-AM3-V1, R69-A69-AM15-V3, R69-A69-AM17-V2, R69-A69-AM30-v1, R70-A70-AM3-V1, R70-A70-AM15-V3, R70-A70-AM17-V2, R70-A70-AM30-v1, R71-A71-AM3-V1, R71-A71-AM15-V3, R71-A71-AM17-V2, R71-A71-AM30-v1, R72-A72-AM1-V1,R72-A72-AM4-V1, R72-A72-AM15-V3, R73-A73-AM1-V1, R73-A73-AM4-V1, R73-A73-AM15-V3,R76-A76-AM1-V1, R76-A76-AM15-V3, R77-A77-AM1-V1, R77-A77-AM15-V3, R78-A78-AM1-V1, R78-A78-AM15-V3, R78-A78-AM8-V1, R79-A79-AM1-V1, R79-A79-AM15-V3, R79-A79-AM8-V1, R80-A80-AM1-V1, R80-A80-AM15-V3, R80-A80-AM8-V1, R81-A81-AM1-V1, R81-A81-AM15-V3, R81-A81-AM8-V1
	3 Alto			R16-A16-AM18-V1, R16-A16-AM18-V2, R17-A17-AM18-V1, R17-A17-AM18-V2, R18-A18-AM18-V1, R18-A18-AM18-V2, R19-A19-AM18-V1, R19-A19-AM18-V2, R20-A20-AM18-V1, R20-A20-AM18-V2, R21-A21-AM18-V1, R21-A21-AM18-V2, R22-A22-AM18-V1, R22-A22-AM18-V2, R23-A23-AM18-V1, R23-A23-AM18-V2, R24-A24-AM18-V1, R24-A16-AM18-V2, R25-A25-AM18-V1, R25-A25-AM18-V2, R26-A26-AM18-V1, R26-A26-AM18-V2, R27-A27-AM18-V1, R27-A27-AM18-V2, R28-A28-AM18-V1, R28-A28-AM18-V2, R29-A29-AM18-V1, R29-A29-AM18-V2, R30-A30-AM18-V1, R30-A30-AM18-V2, R31-A31-AM18-V1, R31-A31-AM18-V2, R32-A32-AM18-V1, R57-A57-AM14-V2

Fuente: Los Autores

9. TRATAMIENTO DE RIESGOS

Teniendo en cuenta el Anexo (A) que relaciona la norma ISO/IEC 27001:2013 tomado como referencia, se procede a realiza la asociación de controles para aplicar a los activos de información que hacen parte de los procesos misionales en la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, estos son relacionados en el cuadro 14 Controles por amenaza, con el propósito de tener una visión más clara y ordenada al momento de realizar el análisis de controles a definir para los activos de información.

9.1 SEGREGACIÓN DE CONTROLES

El siguiente cuadro está conformado por 4 ítems donde se describen los siguientes criterios a tener en cuenta:

- ID AMENAZA: corresponde al código identificador de la amenaza.
- AMENAZA: corresponde a la mención de la amenaza.
- CONTROLES: corresponde a los controles que se aplican a la amenaza.

Cuadro 14. Controles por amenaza

ID Amenaza	Amenaza	Controles			
AM1	Daños por agua o fuego	A.8.1.1 A.8.1.2 A.11.1.1	A.11.1.2 A.11.1.3 A.11.1.4	A.12.3.1 A.12.4.2 A.17.1.1	A.17.1.2 A.17.1.3
AM2	Desastres naturales	A.11.1.3	A.11.1.4	A.11.1.5	
AM3	Corte del suministro eléctrico	A.11.1.1 A.11.1.2	A.11.1.3 A.11.2.1	A.13.1.2 A.15.2.1	A.17.2.1
AM4	Condiciones inadecuadas de temperatura o humedad	A.11.2.2	A.11.1.3	A.11.1.5	
AM5	Errores de los usuarios	A.7.2.2 A.8.1.3 A.8.2.2 A.9.2.3	A.9.3.1 A.9.4.4 A.11.2.7 A.11.2.8	A.11.2.9 A.12.1.1 A.12.2.1 A.12.6.2	A.16.1.6
AM6	Fallo de servicios de comunicaciones	A.13.1.2	A.15.2.1	A.17.2.1	
AM7	Errores del administrador	A.6.1.2 A.8.2.1 A.9.1.2 A.9.2.1 A.9.2.3	A.9.2.5 A.9.2.6 A.9.4.1 A.9.4.3 A.11.2.6	A.12.1.1 A.12.1.2 A.12.4.3 A.12.6.1 A.13.1.1	A.16.1.5 A.16.1.6 A.18.2.3
AM8	Errores de configuración	A.6.1.1 A.17.1.3	A.8.1.1	A.9.2.6	A.15.1.3
AM9	Difusión de software dañino	A.12.5.1	A.12.6.1	A.12.6.2	A.12.7
AM10	Escapes de información	A.7.2.1	A.7.2.3	A.13.2.3	
AM11	Alteración accidental de la información	A.6.1.2	A.9.1.1	A.9.4.1	A.13.1.3
AM12	Destrucción de información	A.6.1.2 A.7.1.1 A.8.1.4 A.9.1.2 A.9.2.3	A.9.2.5 A.9.2.6 A.11.1.1 A.11.1.2 A.11.2.5	A.11.2.8 A.12.1.1 A.12.1.2 A.12.3.1 A.12.4.3	A.15.1.1 A.15.1.2 A.18.1.3

Cuadro 14. (continuación)

ID Amenaza	Amenaza	Controles			
AM13	Fugas de información	A.16.1.1 A.16.1.2	A.16.1.3 A.16.1.6	A.18.1.4 A.7.2.2	A.7.2.3 A.9.3.1
AM14	Vulnerabilidad de los programas	A.6.1.4	A.9.1.2	A.9.4.4	
AM15	Errores de mantenimiento / actualización de programas (software, hardware)	A.8.1.1 A.8.1.2 A.8.2.1	A.8.2.2 A.11.2.4 A.12.1.2	A.12.3.1 A.12.6.1 A.14.1.1	A.15.2.2
AM16	Caída de sistema por agotamiento de recurso	A.9.4.4	A.12.1.2	A.12.1.3	A.12.5.1
AM17	Perdida de equipos	A.8.1.1	A.8.1.2	A.8.1.3	A.8.1.4
AM18	Indisponibilidad del personal	A.7.1.1	A.7.1.2		
AM19	Manipulación de la configuración	A.6.1.1	A.6.1.2	A.6.1.3	A.6.2.2
AM20	Abuso de privilegios de acceso	A.7.2.2 A.7.2.3 A.7.3.1 A.9.1.1	A.9.2.1 A.9.2.3 A.9.2.5 A.9.2.6	A.9.4.1 A.9.4.2 A.12.4.3 A.2.4.1	A.13.1.1
AM21	Uso no previsto	A.7.2.1 A.7.2.2	A.7.2.3 A.8.1.3	A.8.2.1 A.8.2.3	A.11.2.7 A.11.2.1
AM22	Difusión de software dañino	A.7.2.2 A.7.2.3 A.8.3.1	A.9.1.2 A.9.2.3 A.9.4.4	A.12.2.1 A.12.4.1 A.12.5.1	A.12.6.2
AM23	Acceso no autorizado	A.6.1.3 A.6.2.2 A.7.3.1 A.9.1.1 A.9.1.2 A.9.2.2	A.9.2.4 A.9.2.5 A.9.2.6 A.9.3.1 A.9.4.1 A.9.4.2	A.9.4.3 A.11.1.1 A.11.1.2 A.11.1.3 A.11.2.3 A.11.2.8	A.12.4.1 A.12.4.2 A.13.1.1 A.13.1.3
AM24	Modificación deliberada de la información	A.6.1.2 A.6.2.2 A.8.1.2 A.8.2.1 A.9.2.3	A.9.2.5 A.9.2.6 A.9.4.1 A.10.1.1 A.11.1.1	A.11.2.8 A.12.4.1 A.13.1.1 A.13.1.3 A.13.2.2	A.13.2.3 A.14.1.2 A.14.1.3 A.15.1.1 A.18.1.5
AM25	Divulgación de información	A.7.2.2 A.7.2.3	A.7.3.1	A.9.3.1	A.9.4.1
AM26	Manipulación de programas	A.9.4.1 A.9.2.3	A.7.2.3 A.9.2.2	A.9.4.3 A.9.2.5	A.9.4.5
AM27	Manipulación de equipos	A.7.2.3 A.11.2.1	A.11.2.4 A.11.2.5	A.11.2.7 A.11.2.8	A.11.2.9
AM28	Denegación de servicio	A.7.2.3 A.9.1.2	A.9.4.4 A.11.2.3	A.12.1.3 A.16.2.1	
AM29	Robo	A.7.2.3 A.8.1.3	A.9.1.1 A.9.4.2	A.11.2.1 A.11.2.8	A.13.2.4
AM30	Virus	A.7.2.2 A.8.2.3	A.11.2.1 A.11.2.4	A.11.2.7 A.12.2.1	A.16.1.3 A.16.1.7

Fuente. Los autores

Una vez se han identificado los controles para aplicar a los activos de información, se elabora una matriz de tratamiento de riesgos en donde se tendrá como resultado la obtención del riesgo residual. (ver cuadro 15)

Cuadro 15. Tratamiento de riesgos

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
R16	Recurso Humano	3	3	9	AM5-V2	A.7.2.2 Toma de conciencia, educación y formación en seguridad de la información	Se debe crear un programa de capacitación dirigido a los empleados de la organización a fin reforzar los conocimientos en seguridad de la información.	Coordinadora Admin y del SIG, Administrador de sistemas, Asesor de sistemas	Semanas 01 marzo 2021	1	2	2
						A.11.2.9 Política de escritorio y pantalla limpios	Se debe tener un procedimiento con relación a uso de información en pantalla en donde no se podrá almacenar información, únicamente se podrá alojar información en las unidades autorizadas.	Coordinadora Admin y del SIG, Administrador de sistemas, Asesor de sistemas				
						A.12.1.1 Procedimientos de operación documentados	Cada procedimiento que hace parte de los procesos misionales de la Curaduría Urbana No. 3 deben estar previamente documentado y socializado.	Coordinadora Admin y del SIG, Administrador de sistemas, Asesor de sistemas				
						A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	Se es necesario dado a que frente un evento de seguridad presentado se debe evaluar para buscar una mejora en el sistema de gestión de seguridad de la información.	Coordinadora Admin y del SIG, Administrador de sistemas, Asesor de sistemas				
R56	A56	2	3	6	AM24-V1	A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información	Director administrativo, Coordinadora Admin y del SIG, Administrador de sistemas	Semanas 02 marzo 2021	2	2	4
						A.8.2.1 Calificación de la información	La información manejada en el proceso misional se debe clarificar y avalar por la alta Dirección	Director administrativo, Coordinadora Admin y del SIG.				
						A.12.4.1 Registro de eventos	Se debe crear un procedimiento donde se realicen auditorías a los usuarios en relación al uso de los recursos tecnológicos.	Coordinadora adtiva y del SIG				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.8.2.1 Calificación de la información	La información manejada en el proceso misional se debe clarificar y avalar por la alta Dirección	Director administrativo, Coordinadora Admin y del SIG.				
						A.12.4.1 Registro de eventos	Se debe crear un procedimiento donde se realicen auditorías a los usuarios en relación al uso de los recursos tecnológicos.	Coordinadora adtiva y del SIG				
						A.13.1.1 Controles en redes	Es necesario la creación de controles en redes para garantizar la protección de los dispositivos de comunicación.	Coordinadora adtiva y del SIG, Administrador de sistemas, Asesor de sistemas				
						A.13.2.2 Acuerdos sobre trasferencia de información	Es necesario realizar acuerdos de transferencia de información para garantizar un canal de comunicación entre la curaduría urbana No. 3 y clientes y proveedores.	Proveedores, Asesor de sistemas				
						A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas	Se requiere dado a que se la información que se maneja en las aplicaciones misionales debe ser consultada por los usuarios y clientes.	Coordinadora adtiva y del SIG, Administrador de sistemas, Asesor de sistemas				
						A.14.1.3 Protección de transacciones de los servicios de las aplicaciones	Se debe crear un procedimiento donde las transacciones sistemáticas se visualicen para proteger y evitar la trasmisión incompleta.	Administrador de sistemas, Asesor de sistemas				
						A.15.1.1 Política de la seguridad de la información para las relaciones con proveedores	Se debe definir los procedimientos en donde se tenga claras lar las responsabilidades que se tienen con relación a proveedores.	Coordinadora adtiva y del SIG, Administrador de sistemas, Asesor de sistemas				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
		3	2	6	AM10-V1	A.7.2.1 Responsabilidades de la Dirección	La Dirección de la organización debe aprobar y velar por el cumplimiento de las políticas de seguridad de la información.	Director administrativo	Semanas 03 marzo 2021	1	2	2
						A.7.2.3 Proceso disciplinario	Se deben tomar acciones disciplinarias a funcionarios quienes incurran en hechos donde se vea comprometida la integridad, confidencialidad y disponibilidad de la información.	Director administrativo				
						A.13.2.3 Mensajería Electrónica	Se debe garantizar la información que es utilizada por canales como correo electrónico en relación e la disponibilidad integridad y confidencialidad.	Administrador de sistemas				
		2	3	6	AM17-V2	A.8.1.1 Inventario de Activos	Los activos de información que conforman los procesos misionales deben estar previamente identificados y consignados un una bitácora o software de gestión de activos.	Coordinadora adtiva y del SIG, Administrador de sistemas	Semanas 04 marzo 2021	1	1	1
						A.8.1.2 Propiedad de los activos	Se debe establecer la persona que es responsable del activo de información.	Profesional gestión adtiva.				
						A.8.1.3 Uso Aceptable de los activos	Se debe definir un procedimiento para el uso adecuado de los activos de información.	Coordinadora adtiva y del SIG, Administrador de sistemas				
						A.8.1.4 Devolución de los activos	Se debe consignar en un medio los activos de información que se devuelven por parte de un funcionario al momento de finalizar su contrato con la organización a fin de generar una paz y salvo.	Administrador de sistemas, Profesional gestión adtiva.				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
		2	3	6	AM11-V2	A.9.4.1 Restricción de acceso a la información.	La Dirección de la organización debe velar por el cumplimiento de la política de la gestión de accesos.	Director administrativo	Semana 01 abril 2021Ss			
						A.13.1.3 Separación en redes	Una vez se definen roles se debe proteger el acceso a la información de la que hacen uso los funcionarios de la Curaduría Urbana No. 3.	Administrador de sistemas				
		2	3	6	AM-29-V1	A.7.2.3 Proceso disciplinario	Se deben tomar acciones disciplinarias a funcionarios quienes incurran en hechos donde se vea comprometida la integridad, confidencialidad y disponibilidad de la información.	Profesional gestión adtiva.	Semana 02 abril 2021	1	2	2
						A.9.4.2 Procedimiento de ingreso seguro.	Se debe consignar mediante documento la entrega de contraseñas a usuarios de manera personal a fin de garantizar la entrega formal de manera confidencial.	Coordinadora adtiva y del SIG, Administrador de sistemas.				
						A.13.2.4 Acuerdos de confidencialidad o de no divulgación	Se debe tener consignado los acuerdos de confidencialidad entre clientes proveedores y empleados de la Curaduría urbana No. 3	Profesional gestión adtiva.				
R57	A57	3	3	9	AM14-V2	A.9.1.2 Acceso a redes y servicios es red	Se definir unos roles de acceso de acuerdo al cargo y área que conforman los procesos misionales la política de uso de los activos de información.	Coordinadora adtiva y del SIG, Administrador de sistemas.	Semana 03 abril 2021	1	2	2
						A.9.4.4 Uso de programas utilitarios privilegiados	Se deben definir que programas utilitarios son autorizados para uso a en los procesos misionales, estos deben tener el VoBo de la Gerencia.	Coordinadora adtiva y del SIG, Administrador de sistemas.				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
		2	3	6	AM5-V2	A.7.2.2 Toma de conciencia educación y formación en seguridad de la información.	Se debe crear un programa de capacitación dirigido a los empleados de la organización a fin reforzar los conocimientos en seguridad de la información.	Coordinadora adtiva y del SIG, Administrador de sistemas.	Semana 04 abril 2021	2	2	4
						A.8.1.3 Uso Aceptable de los activos.	Se debe definir un procedimiento para el uso adecuado de los activos de información.	Coordinadora adtiva y del SIG, Administrador de sistemas.				
						A.9.2.3 Gestión de derechos de acceso privilegiado	Se debe definir claramente que usuarios deben tener acceso con privilegios a los activos de información de la Curaduría Urbana No.3	Coordinadora adtiva y del SIG, Administrador de sistemas				
						A.9.3.1 Uso de la información de autenticación secreta	Por parte de la Dirección de la organización se debe velar por el cumplimiento de la política de uso de los activos de información	Coordinadora adtiva y del SIG, Administrador de sistemas				
						A.11.2.8 Equipos de usuario desatendido	Se debe garantizar que los activos de información de la organización se encuentran en condiciones óptimas aun cuando estos no se encuentres supeditados a supervisión por parte del líder de área	Administrador de Sistemas, Asesor de Sistemas.				
						A.12.1.1 Procedimientos de operación documentados	Cada procedimiento que hace parte de los procesos misionales de la Curaduría Urbana No. 3 deben estar previamente documentado y socializado	Coordinadora adtiva y del SIG, Administrador de sistemas				
						A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	Se es necesario dado a que frente un evento de seguridad presentado se debe evaluar para buscar una mejora en el sistema de gestión de seguridad de la información	Coordinadora adtiva y del SIG, Administrador de sistemas, Usuarios finales				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
		2	3	6	AM11-V1	A.6.1.2 Separación de deberes	Se tiene definidas las áreas en los procesos misionales.	Coordinadora adtiva y del SIG.	Semana 01 mayo 2021	1	2	2
						A.9.1.1 Política de control de acceso	Se debe crear una política para el control de acceso a los activos de información de la Curaduría Urbana N.3.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.9.4.1 Restricción de acceso a la información	La Dirección de la organización debe velar por el cumplimiento de la política de la gestión de accesos.	Director administrativo.				
		2	3	6	AM15-V3	A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información	Coordinadora adtiva y del SIG, Asesor de sistemas	Semana 02 mayo 2021	2	2	4
						A.8.2.1 Calificación de la información	La información manejada en el proceso misional se debe clarificar y avalar por la alta Dirección	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.12.1.2 Gestión de cambios	Los cambios que se realicen en la organización a nivel de proceso deben estar controlados para fines pertinentes	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.12.3.1 Respaldo de la información	Se debe garantizar el respaldo de la información en caso de que esta se vea comprometida ante un evento de disponibilidad, o daño adicional garantiza	Asesor Sistemas, Administrador de Sistemas				
						A.12.6.1 Gestión de las vulnerabilidades técnicas	Se requiere tener un procedimiento de acción para validar información ante posibles amenazas informáticas	Asesor Sistemas, Administrador de Sistemas				
R58	A58	2	3	6	AM15-V3	A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información	Coordinadora adtiva y del SIG, Asesor de sistemas.		2	2	4

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.12.1.2 Gestión de cambios	Los cambios que se realicen en la organización a nivel de proceso deben estar controlados para fines pertinentes.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.12.3.1 Respaldo de la información	Se debe garantizar el respaldo de la información en caso de que esta se vea comprometida ante un evento de disponibilidad, o daño adicional garantiza.	Asesor Sistemas, Administrador de Sistemas				
						A.12.6.1 Gestión de las vulnerabilidades técnicas	Se requiere tener un procedimiento de acción para validar información ante posibles amenazas informáticas.	Asesor Sistemas, Administrador de Sistemas				
		2	3	6	AM28-V1	A.9.1.2 Acceso a redes y servicios es red	Se definir unos roles de acceso de acuerdo al cargo y área que conforman los procesos misionales	Asesor Sistemas, Administrador de Sistemas	Semana 03 mayo 2021	2	1	2
						A.9.4.4 Uso de programas utilitarios privilegiados	Se deben definir que programas utilitarios son autorizados para uso a en los procesos misionales, estos deben tener el VoBo de la Gerencia	Asesor Sistemas, Administrador de Sistemas				
						A.11.2.3 Seguridad del cableado	Se debe garantizar que el cableado estructurado de la organización se encuentre certificado para garantizar la trasmisión de datos voz	Asesor Sistemas, Administrador de Sistemas				
						A.12.1.3 Gestión de la capacidad	Se debe realizar auditorías a la infraestructura de la organización a fin de garantizar la capacidad tecnológica de la organización	Asesor Sistemas, Administrador de sistemas, Coordinadora adtiva y del SIG				
R61	A61	2	3	6	AM15-V3	A.8.1.1 Inventario de Activos	Los activos de información que conforman los procesos misionales deben estar previamente identificados y consignados un una bitácora o software de gestión de activos	Asesor Sistemas	Semana 04 mayo 2021	2	2	4

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.12.1.2 Procedimientos de operación documentados	Cada procedimiento que hace parte de los procesos misionales de la Curaduría Urbana No. 3 deben estar previamente documentado y socializado.	Coordinadora adtiva y del SIG, Asesor Sistemas				
						A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	Se hace necesaria la aplicación en relación a la adquisición de tecnología que se adhiere a los procesos misionales de la Curaduría Urbana No.3.	Asesor Sistemas				
		2	3	6	AM16-V1	A.12.1.2 Gestión de cambios	Los cambios que se realicen en la organización a nivel de proceso deben estar controlados para fines pertinentes.	Coordinadora adtiva y del SIG, Asesor de sistemas	Semana 01 junio 2021	2	2	4
						A.12.1.3 Gestión de la capacidad	Se debe realizar auditorías a la infraestructura de la organización a fin de garantizar la capacidad tecnológica de la organización.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.12.5.1 Instalación de software y sistemas operativos	Se debe contar con un procedimiento donde se especifique la instalación de sistemas operativos y software, lo anterior debe estar avalado por la Gerencia de la organización.	Administrador de Sistemas				
R63-R71	Hadware PC	2	3	6	AM3-V1	A.11.1.1 Perímetro de seguridad física	Se debe tener un control de acceso a las instalaciones de la Curaduría Urbana No3, así mismo debe tener un control a las áreas de la organización donde se esté gestionando información de la organización	Coordinadora adtiva y del SIG	Semana 02 junio 2021	2	2	4
						A.11.1.2 Controles de acceso físicos.	Se debe tener un control biométrico para ingresar a las instalaciones y áreas de la organización, así mismo los empleados deben estar plenamente identificados por medio de Carnets	Coordinadora adtiva y del SIG				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.11.1.3 Seguridad de oficinas recintos e instalaciones.	La instalación de la organización y áreas deben estar dotadas de elementos de seguridad en caso de emergencia	Coordinadora adtiva y del SIG				
						A.11.2.1 Ubicación y protección del equipo	Los equipo o activos de información deben estar en un lugar adecuado en donde no estén expuestos a daños físicos	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.13.1.2 Seguridad en los servicios de red.	Se requiere dado a que se debe garantizar la disponibilidad de los servicios para el funcionamiento del Core de negocio	Asesor de sistemas				
						A.15.2.1 Seguimiento y revisión de los servicios de los proveedores.	seguimiento a los servicios ofrecidos, contratados y ejecutados en donde se interactúe con la seguridad informática	Coordinadora adtiva y del SIG				
						A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.	Se requiere dado a que se debe garantizar la disponibilidad de los sistemas de comunicación que realizan procesamiento de información en la curaduría Urbana No.3	Asesor de sistemas				
		3	3	9	AM5-V2	A.7.2.2 Toma de conciencia educación y formación en seguridad de la información	Se debe crear un programa de capacitación dirigido a los empleados de la organización a fin reforzar los conocimientos en seguridad de la información	Coordinadora adtiva y del SIG, Asesor de sistemas	Semana 03 junio 2021	1	2	2
						A.11.2.9 Política de escritorio y pantalla limpia	Se debe tener un procedimiento en relación a uso de información en pantalla en donde no se podrá almacenar información, únicamente se podrá alojar información en las unidades autorizadas.	Administrador Sistemas				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.12.1.1 Procedimientos de operación documentados	Cada procedimiento que hace parte de los procesos misionales de la Curaduría Urbana No. 3 deben estar previamente documentado y socializado.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	Se es necesario dado a que frente un evento de seguridad presentado se debe evaluar para buscar una mejora en el sistema de gestión de seguridad de la información	Coordinadora adtiva y del SIG, Asesor de sistemas.				
		2	3	6	AM15-V3	A.8.1.1 Inventario de Activos	Los activos de información que conforman los procesos misionales deben estar previamente identificados y consignados un una bitácora o software de gestión de activos	Coordinadora adtiva y del SIG, Asesor de sistemas	Semana 04 junio 2021	1	2	2
						A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.2.1 Calificación de la información	La información manejada en el proceso misional se debe clarificar y avalar por la alta Dirección.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.2.2 Etiquetado de la Información	Se debe crear un procedimiento para etiquetar la información avalado por la Dirección de la organización	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.11.2.4 Mantenimiento de equipos	Se debe contar con un cronograma de mantenimiento de equipos anual a fin de garantizar el correcto funcionamiento del activo de información	Asesor de sistemas				
						A.12.3.1 Respaldo de la información	Se debe garantizar el respaldo de la información en caso de que esta se vea comprometida ante	Asesor de sistemas, Administrados Sistemas				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
							un evento de disponibilidad, o daño adicional garantiza					
						A.12.6.1 Gestión de las vulnerabilidades técnicas	Se requiere tener un procedimiento de acción para validar información ante posibles amenazas informáticas	Asesor de sistemas, Administrados Sistemas				
						A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	Se hace necesaria la aplicación en relación a la adquisición de tecnología que se adhiere a los procesos misionales de la Curaduría Urbana No.3	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.15.2.2 Gestión de cambios en los servicios de los proveedores	Se debe auditar y validar los cambios que un proveedor de servicio realice a fin de garantizar el flujo de la operación sin comprometer la seguridad informática	Coordinadora adtiva y del SIG, Asesor de sistemas				
		2	3	6	AM17-V2	A.8.1.1 Inventario de Activos	Los activos de información que conforman los procesos misionales deben estar previamente identificados y consignados un una bitácora o software de gestión de activos	Coordinadora adtiva y del SIG	Semana 01 Julio 2021	2	2	4
						A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.1.4 Devolución de los activos	Se debe consignar en un medio los activos de información que se devuelven por parte de un funcionario al momento de finalizar su contrato con la organización a fin de generar una paz y salvo.	Coordinadora adtiva y del SIG				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
		2	3	6	AM30-v1	A.7.2.2 Toma de conciencia educación y formación en seguridad de la información	Se debe crear un programa de capacitación dirigido a los empleados de la organización a fin reforzar los conocimientos en seguridad de la información	Coordinadora adtiva y del SIG, Asesor de sistemas Usuarios Finales	Semana 02 julio 2021	2	1	2
						A.8.2.3 Manejo de activos	Se debe crear un procedimiento para el manejo de los activos de información	Coordinadora adtiva y del SIG				
						A.11.2.1 Ubicación y protección del equipo	Los equipo o activos de información deben estar en un lugar adecuado en donde no estén expuestos a daños físicos	Coordinadora adtiva y del SIG				
						A.11.2.4 Mantenimiento de equipos	Se debe contar con un cronograma de mantenimiento de equipos anual a fin de garantizar el correcto funcionamiento del activo de información	Asesor de sistemas, Administrados Sistemas				
						A.11.2.7 Disposición segura o reutilización de equipos	Se debe tener un procedimiento donde se relaciones el software instalado antes de reutilizarse o ponerse en reusó	Coordinadora adtiva y del SIG, Asesor de sistemas, Administrados Sistemas				
						A.12.2.1 Controles contra códigos maliciosos	Se debe tener una solución tecnológica para detección de código malicioso y su mitigación, adicional socializar con los funcionarios de la organización sobre el tratamiento y manejo que se debe dar.	Asesor de sistemas, Administrados Sistemas				
						A.16.1.3 Reporte de debilidades de seguridad de la información	Se debe tener un procedimiento de actualización frente a un evento de seguridad, así mismo se debe consignar el evento para un posterior análisis.	Asesor de sistemas, Administrados Sistemas				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.16.1.7 Recolección de evidencias	Se requiere dado a que si se tiene una evidencia física se debe reportar ante las autoridades competentes para efectos dentro de un marco legal.	Coordinadora adtiva y del SIG, Asesor de sistemas, Administrados Sistemas				
R72-R73	Hadware Servidor	2	3	6	AM1-V1	A.8.1.1 Inventario de Activos	Los activos de información que conforman los procesos misionales deben estar previamente identificados y consignados un una bitácora o software de gestión de activos.	Coordinadora adtiva y del SIG, Asesor de sistemas, Administrados Sistemas	Semana 03 julio 2021	2	2	4
						A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información.	Coordinadora adtiva y del SIG				
						A.11.1.2 Controles de acceso Físicos	Se debe tener un control biométrico para ingresar a las instalaciones y áreas de la organización, así mismo los empleados deben estar plenamente identificados por medio de carnés.	Coordinadora adtiva y del SIG				
						A.11.1.3 Seguridad de oficinas recintos e instalaciones	La instalación de la organización y áreas deben estar dotadas de elementos de seguridad en caso de emergencia.	Coordinadora adtiva y del SIG				
						A.11.1.4 Protección contras amenazas externas y ambientales	Se debe contar con un protocolo al momento de presentarse un evento de seguridad donde se vea comprometidas las áreas y activos de información.	Coordinadora adtiva y del SIG, Asesor de sistemas, Administrados Sistemas				
						A.12.3.1 Respaldo de la información	Se debe garantizar el respaldo de la información en caso de que esta se vea comprometida ante un evento de disponibilidad, o daño adicional garantiza.	Asesor de sistemas, Administrados Sistemas				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.17.1.1 Planificación de la continuidad de la seguridad de la información	Se requiere dado que se debe garantizar la continuidad del negocio y las operaciones ante un evento o incidente de seguridad.	Coordinadora adtiva y del SIG, Asesor de sistemas, Administrados Sistemas				
		2	3	6	AM4-V1	A.11.1.3 Seguridad de oficinas recintos e instalaciones.	La instalación de la organización y áreas deben estar dotadas de elementos de seguridad en caso de emergencia.	Director administrativo.	Semana 04 julio 2021	2	1	2
						A.11.1.5 Trabajo en áreas seguras.	Se debe contar con un procedimiento que permita establecer el uso de trabajo en las áreas donde se está gestionado información de la organización de manera segura.	Asesor de sistemas, director administrativo.				
		2	3	6	AM15-V3	A.8.1.1 Inventario de Activos	Los activos de información que conforman los procesos misionales deben estar previamente identificados y consignados un una bitácora o software de gestión de activos.	Coordinadora adtiva y del SIG, Asesor de sistemas	Semana 01 agosto 2021	1	2	2
						A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.2.1 Calificación de la información	La información manejada en el proceso misional se debe clarificar y avalar por la alta Dirección.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.2.2 Etiquetado de la Información	Se debe crear un procedimiento para etiquetar la información avalado por la Dirección de la organización.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.11.2.4 Mantenimiento de equipos	Se debe contar con un cronograma de mantenimiento de equipos anual a fin de garantizar el correcto funcionamiento del activo de información.	Asesor de sistemas				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.12.3.1 Respaldo de la información	Se debe garantizar el respaldo de la información en caso de que esta se vea comprometida ante un evento de disponibilidad, o daño adicional garantiza.	Asesor de sistemas, Administrados Sistemas				
						A.12.6.1 Gestión de las vulnerabilidades técnicas	Se requiere tener un procedimiento de acción para validar información ante posibles amenazas informáticas	Asesor de sistemas, Administrados Sistemas				
						A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	Se hace necesaria la aplicación en relación a la adquisición de tecnología que se adhiere a los procesos misionales de la Curaduría Urbana No.3.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.15.2.2 Gestión de cambios en los servicios de los proveedores	Se debe auditar y validar los cambios que un proveedor de servicio realice a fin de garantizar el flujo de la operación sin comprometer la seguridad informática.	Coordinadora adtiva y del SIG, Asesor de sistemas				
R76-R77	A76-A77	2	3	6	AM1-V1	A.8.1.1 Inventario de Activos	Los activos de información que conforman los procesos misionales deben estar previamente identificados y consignados un una bitácora o software de gestión de activos.	Coordinadora adtiva y del SIG, Asesor de sistemas, Administrados Sistemas	Semana 02 Agosto 2021	2	2	4
						A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información.	Coordinadora adtiva y del SIG				
						A.11.1.2 Controles de acceso Físicos	Se debe tener un control biométrico para ingresar a las instalaciones y áreas de la organización, así mismo los empleados deben estar plenamente identificados por medio de carnés.	Coordinadora adtiva y del SIG				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.11.1.3 Seguridad de oficinas recintos e instalaciones	La instalación de la organización y áreas deben estar dotadas de elementos de seguridad en caso de emergencia.	Coordinadora adtiva y del SIG				
						A.11.1.4 Protección contras amenazas externas y ambientales	Se debe contar con un protocolo al momento de presentarse un evento de seguridad donde se vea comprometidas las áreas y activos de información.	Coordinadora adtiva y del SIG, Asesor de sistemas, Administrados Sistemas				
						A.12.3.1 Respaldo de la información	Se debe garantizar el respaldo de la información en caso de que esta se vea comprometida ante un evento de disponibilidad, o daño adicional garantiza.	Asesor de sistemas, Administrados Sistemas				
		2	3	6	AM15-V3	A.8.1.1 Inventario de Activos	Los activos de información que conforman los procesos misionales deben estar previamente identificados y consignados un una bitácora o software de gestión de activos.	Coordinadora adtiva y del SIG, Asesor de sistemas	Semana 03 Agosto 2021	2	2	4
						A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.2.1 Calificación de la información	La información manejada en el proceso misional se debe clarificar y avalar por la alta Dirección.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.2.2 Etiquetado de la Información	Se debe crear un procedimiento para etiquetar la información avalado por la Dirección de la organización.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.11.2.4 Mantenimiento de equipos	Se debe contar con un cronograma de mantenimiento de equipos anual a fin de garantizar el correcto funcionamiento del activo de información.	Asesor de sistemas				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.12.3.1 Respaldo de la información	Se debe garantizar el respaldo de la información en caso de que esta se vea comprometida ante un evento de disponibilidad, o daño adicional garantiza.	Asesor de sistemas, Administrados Sistemas				
						A.12.6.1 Gestión de las vulnerabilidades técnicas	Se requiere tener un procedimiento de acción para validar información ante posibles amenazas informáticas	Asesor de sistemas, Administrados Sistemas				
						A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	Se hace necesaria la aplicación en relación con la adquisición de tecnología que se adhiere a los procesos misionales de la Curaduría Urbana No.3.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.15.2.2 Gestión de cambios en los servicios de los proveedores	Se debe auditar y validar los cambios que un proveedor de servicio realice a fin de garantizar el flujo de la operación sin comprometer la seguridad informática.	Coordinadora adtiva y del SIG, Asesor de sistemas				
R78-R81	A78-A81	2	3	6	AM1V1	A.8.1.1 Inventario de Activos	Los activos de información que conforman los procesos misionales deben estar previamente identificados y consignados un una bitácora o software de gestión de activos.	Coordinadora adtiva y del SIG, Asesor de sistemas, Administrados Sistemas	Semana 04 agosto 2021	1	3	3
						A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información.	Coordinadora adtiva y del SIG				
						A.11.1.2 Controles de acceso Físicos	Se debe tener un control biométrico para ingresar a las instalaciones y áreas de la organización, así mismo los empleados deben estar plenamente identificados por medio de carnés.	Coordinadora adtiva y del SIG				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.11.1.3 Seguridad de oficinas recintos e instalaciones	La instalación de la organización y áreas deben estar dotadas de elementos de seguridad en caso de emergencia.	Coordinadora adtiva y del SIG				
						A.11.1.4 Protección contras amenazas externas y ambientales	Se debe contar con un protocolo al momento de presentarse un evento de seguridad donde se vea comprometidas las áreas y activos de información.	Coordinadora adtiva y del SIG, Asesor de sistemas, Administrados Sistemas				
						A.12.3.1 Respaldo de la información	Se debe garantizar el respaldo de la información en caso de que esta se vea comprometida ante un evento de disponibilidad, o daño adicional garantiza.	Asesor de sistemas, Administrados Sistemas				
		2	3	6	AM15-V3	A.8.1.1 Inventario de Activos	Los activos de información que conforman los procesos misionales deben estar previamente identificados y consignados un una bitácora o software de gestión de activos.	Coordinadora adtiva y del SIG, Asesor de sistemas	Semana 01 septiembre 2021	2	2	4
						A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.2.1 Calificación de la información	La información manejada en el proceso misional se debe clarificar y avalar por la alta Dirección.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.2.2 Etiquetado de la Información	Se debe crear un procedimiento para etiquetar la información avalado por la Dirección de la organización.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.1.1 Inventario de Activos	Los activos de información que conforman los procesos misionales deben estar previamente identificados y consignados un una bitácora o software de gestión de activos.	Coordinadora adtiva y del SIG, Asesor de sistemas				

Cuadro 15. (Continuación)

ID riesgo	ID activos / tipo de activo	Probabilidad	Impacto	Nivel de riesgo inherente	Amenazas	Controles	Tratamiento	Responsable	Fecha	Probabilidad	Impacto	Nivel de riesgo residual
						A.8.1.2 Propiedad de los activos	Se debe establecer que persona es el responsable del activo de información.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.2.1 Calificación de la información	La información manejada en el proceso misional se debe clarificar y avalar por la alta Dirección.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.8.2.2 Etiquetado de la Información	Se debe crear un procedimiento para etiquetar la información avalado por la Dirección de la organización.	Coordinadora adtiva y del SIG, Asesor de sistemas				
						A.15.2.2 Gestión de cambios en los servicios de los proveedores	Se debe auditar y validar los cambios que un proveedor de servicio realice a fin de garantizar el flujo de la operación sin comprometer la seguridad informática.	Coordinadora adtiva y del SIG, Asesor de sistemas				
		2	6	6	AM8-V1	A.6.1.1 Roles y responsabilidades para la seguridad de la información.	Se deben definir roles y responsabilidades para el proceso misional de la Curaduría Urbana No.3		Semana 02 septiembre 2021	1	2	2
						A.9.2.6 Retiro o ajuste de los derechos de acceso.	Se debe crear un procedimiento donde se especifique el tratamiento o gestión de los usuarios cuando ya no están vinculados a la Curaduría Urbana No. 3 en calidad de empleados					
						A.15.1.3 Cadena de suministro de tecnología de información y comunicación.	Se requiere hacer un seguimiento a los servicios ofrecidos, contratados y ejecutados en donde se interactúe con la seguridad informática					
						A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Los procedimientos establecidos deben ser eficaces en relación de garantizar el flujo en la operación y la continuidad					

Fuente. Los autores

9.2 RESULTADO RESIDUAL

El riesgo residual es el resultado de aplicar el tratamiento de riesgos a los activos de información críticos de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón, este resultado se debe comparar inicialmente contra la valoración de riesgo inherente, aplicando el tratamiento de riesgos se visualiza una reducción de riesgo la cual tiene un criterio de aceptación por parte de la Dirección Administrativa pactada en el numeral 9.2.5 ACEPTACION DE LOS RIESGOS, posteriormente el riesgo residual se apalanca con la implementación de directrices de seguridad lo que permite mitigar efectos donde se vulnere o se vea comprometida la seguridad de la información.

10. CREACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Con el propósito de establecer las políticas a nivel de seguridad de la información en la curaduría Urbana No.3 Arq. Ana María Cadena Tobón, se presentó a la alta Gerencia los siguientes lineamientos a fin de garantizar los objetivos de negocio de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón dando un manejo en gestión en relación con los riesgos identificados, garantizando y asegurando los activos de información. Es compromiso de la Alta Gerencia hacer cumplir dichos lineamientos para que el sistema de gestión de seguridad de la información en cumplimiento con los objetivos se mantenga en el tiempo.

Los lineamientos establecidos se tomaron como referencia del documento MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFOMACIÓN de la presidencia de la Republica de Colombia a fin de tener un criterio amplio en la creación de los lineamientos.

A continuación, se esbozan los elementos de una política de seguridad de la información, y de acuerdo con ellos, acto seguido se presenta la creación de las políticas de seguridad de la información la para la curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

10.1 ELEMENTOS DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

10.1.1 Objetivo. Crear políticas de seguridad de la información aplicadas a los procesos misionales en la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón con base en la Norma ISO/IEC 27001:2013 que permitan mitigar los riesgos en los activos de información.

10.1.1.1 Alcance. Las políticas relacionadas aplican a los procesos misionales (emisión de conceptos, radicación, estudios técnicos, expedición entrega y notificación de licenciamiento urbanístico) con relación a los activos de información, recurso humano y proveedores.

10.1.1.2 Generalidad. La notificación de las políticas de seguridad se debe socializar a nivel general para su cumplimiento haciendo uso de estrategias que permitan a los usuarios tener una claridad con relación a las mejores prácticas al momento de intervenir en los procesos misionales con los activos de información, el apoyo para hacer cumplir estos lineamientos por parte de la Gerencia y la cultura a los usuarios, son elementos de vital importancia para su mantención.

10.1.1.3 Desarrollo de directrices de seguridad de la información. En un contexto organizacional el cumplimiento de las directrices de seguridad se adhiere un sentido de responsabilidad por parte de todos los funcionarios de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

- Dentro de las juntas organizacionales, se debe crear un comité se gestión de seguridad, cuyo propósito debe recaer sobre en relación con la constate auditoria del sistema de gestión de seguridad de la información.

- El comité de gestión de seguridad debe estar conformado por un representante o líder de las áreas de Concepto de Emisión, Radicación, Estudios Técnicos, Expedición entrega y notificación, Director Administrativo, Coordinador Calidad y asesor de sistemas, quienes mensualmente se reunirán para evaluar los planes de trabajo y las mejoras que surjan durante el desarrollo del Sistema de Gestión de Seguridad de la Información en aras de buscar una mejora continua.

- La Curaduría Urbana No3 Arq. Ana María Cadena Tobón debe integrar a los proveedores quienes suplen de servicios a la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón, el propósito debe ser el evaluar la calidad de los servicios ofertados y si estos están sujetos a cambios, de ser así, se debe levantar un acta relacionando los motivos para ser presentados en comités organizacionales para tomar decisiones.

- La Curaduría Urbana No.3 Arq. Ana María Cadena Tobón debe dotar de recursos tecnológicos a los funcionarios que hacen parte de los procesos misionales en los que ellos interactúan con alguna tecnología haciendo uso de los activos de información, así mismo estos deben estar relacionados mediante un documento en donde se especifique que activo de información se le asigna, este debe ser firmado en mutuo acuerdo entre el funcionario, el Director Administrativo, la Coordinación del Dpto. de Calidad y el Asesor de Sistemas.

- Se debe elaborar un documento llamado hoja de ruta paz y salvo, el propósito de este documento tiene como fin asegurar que al momento de finalizar un contrato entre el empleado y la Curaduría Urbana No.3 Arq. Ana Mara Cadena Tobón, el empleado realice la entrega de los activos de información que se asignaron al momento de hacer parte de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón en calidad de empleado, para ello este formato debe ir firmado en orden cronológico por el Director Administrativo, Coordinación de Calidad y Asesor de sistemas a quien se entregara el equipo asignado para el ejercicio de las funciones propias del cargo.

- La Curaduría Urbana No.3 Arq. Ana María Cadena Tobón debe elaborar una matriz de usuarios y responsabilidades en donde se debe visualizar de una manera clara cuáles son los roles de los funcionarios, estos se deben actualizar mensualmente a fin de realizar los ajustes pertinentes.

- La Curaduría Urbana No.3 Arq. Ana María Cadena Tobón debe elaborar una matriz en donde se relacionen los activos de información de una manera clara separando los activos de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón

frente a los activos de información de los cuales son dueños los proveedores de servicio, esta matriz debe ser actualizada trimestralmente.

- Cuando por necesidad del negocio se adhiera otra área organizacional a los procesos misionales, esta debe tener una cobertura inmediata en relación al Sistema de Gestión de Seguridad de la Información, para ello se debe contar con un plan de adición al sistema.

- La Curaduría Urbana No.3 Arq. Ana María Cadena Tobón debe estar comprometida con la protección en todas sus formas de los activos de información que hacen parte de los procesos misionales, a fin de garantizar la Integridad, Disponibilidad y Confidencialidad en aras de garantizar los objetivos estratégicos del negocio.

- La Curaduría Urbana No.3 Arq. Ana María Cadena Tobón debe crear un proceso de inducción y sensibilización, toda vez que una persona haga parte de los procesos misionales en calidad de empleado, lo anterior con el propósito de crear cultura desde el inicio de su proceso laboral.

- Los incidentes reportados se deben consignar en un documento como lección aprendida, luego de realizar un tratamiento pertinente, se debe socializar con los funcionarios que hacen parte de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón en los procesos misionales con el propósito de tener una visión de acción en caso de presentarse nuevamente un evento.

- La Curaduría Urbana No.3 Arq. Ana María Cadena Tobón debe garantizar que las instalaciones donde reposa los activos de información sean las adecuadas y cumplan con los lineamientos técnicos para preservación de estos.

- La Curaduría Urbana No.3 Arq. Ana María Cadena Tobón debe contratar proveedores externos encargados de realizar pruebas de vulnerabilidades sobre las tecnologías que se utilizan al interior de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón con el propósito de tomar acciones correctivas ante eventos de seguridad que se puedan presentar.

- La Curaduría Urbana No.3 Arq. Ana María Cadena Tobón debe realizar una jornada semestral en la que se pueda realizar una evaluación de la efectividad de controles implementados, a fin de realizar cambios si se requieren.

- Las campañas de concienciación se convierten en una estrategia que pone en contexto a los funcionarios de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, por tal motivo, estas jornadas de sensibilización se deben mantener en el tiempo innovando la manera de socializar las temáticas, para ello es importante que bimensualmente se realicen estas actividades.

- Luego de realizar las jornadas de sensibilización pertinentes en donde los usuarios ya tengan un contexto claro con relación al Sistema de Gestión de Seguridad de la Información, ellos ya deben estar en la capacidad de poder identificar, notificar y actuar frente a un evento de seguridad donde se vea comprometida la seguridad de la información.

10.1.1.4 Atributos de responsabilidades. Dentro del contexto organizacional al interior de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, se establecen roles y responsabilidades en relación con la ejecución de tareas adheridas al Sistema de Gestión de Seguridad de la Información las cuales se mencionan jerárquicamente a continuación:

Director Admirativo. Debe estar comprometido asegurando el cumplimiento es su totalidad del Sistema de Gestión de Seguridad de la Información realizando labores de auditoría interna, trasmitiendo un cambio de cultura organizacional de cara a todos los actores que hacen parte del SGSI interna y externamente, adicional debe:

- Aprobar la matriz de roles y responsabilidades con el propósito de tener un panorama claro en relación con las funciones que ejercen los funcionarios que hacen parte de los procesos misionales al interior de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

- Crear estrategias que permitan mantener en el tiempo el Sistema de Gestión de Seguridad de la Información de cara a los procesos misionales y adheridos a los procesos estratégicos del negocio.

- Avalar los procesos disciplinarios que se apliquen a los funcionarios cuando se vea comprometa la seguridad de la información y que conlleven a la aplicación de estamentos legales.

- Avalar un presupuesto semestral exclusivo para el desarrollo de estrategias comunicativas que permitan generar en los usuarios un cambio de cultura organizacional en relación con el Sistema de Gestión de Seguridad de la Información.

- Garantizar que los activos de información se encuentren debidamente identificados y clasificados por medio de un inventario tecnológico.

Coordinador Sistema Integrado de Gestión (SIG). Debe velar por hacer cumplir los objetivos del Sistema de Gestión de Seguridad de la Información, garantizando que todos los procesos se encuentren correctamente documentados, avalados y aprobados por la Dirección Administrativa, Asesor de sistemas y líderes de área que hacen parte de los procesos misionales, los anterior para efectos de auditorías externas, a su vez es el encargado de programar seguimientos internos apoyado

acciones y planes de trabajo los cuales deberán ser presentados a la Dirección Administrativa en aras de buscar las mejoras continuas que exige la mantención del sistema.

Asesor de Sistemas. Debe velar por hacer cumplir los objetivos del Sistema de Gestión de Seguridad de la Información, es el responsable de diseñar las estrategias tecnológicas a fin de salvaguardar los activos de información garantizando la Integridad, Disponibilidad y Confidencialidad, adicional debe crear los mecanismos que permitan tener una continuidad de negocio en caso tal de ver comprometidos los activos tecnológicos de información, será el responsable de evaluar los servicios ofertados por terceros (proveedores) en relación a lo adquirido por la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón, validando que estos cumplan con el portafolio ofrecido, asimismo será el responsable de reportar a la Dirección Administrativa cualquier evento donde se comprometa la seguridad de la información.

Administrador de Sistemas. Debe velar por hacer cumplir los objetivos del Sistema de Gestión de Seguridad de la Información, será el encargado de crear los usuarios en las plataformas tecnológicas de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón de acuerdo a como estén definidas dentro de la matriz de roles y responsabilidades, el administrador de sistemas debe garantizar el óptimo funcionamiento de la red y a su vez debe reportar al Asesor de sistemas cualquier evento de seguridad en donde se vea comprometida la seguridad de la información.

Auxiliar de Talento Humano. Debe velar por hacer cumplir los objetivos del Sistema de Gestión de Seguridad de la Información, será el encargado de garantizar que el talento humano que hace parte de los procesos misionales en la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón es el idóneo para la ejecución de los cargos y funciones asignadas, deberá aplicar las medidas disciplinarias en relación a los funcionarios cuando se vea comprometida la seguridad de la información, deberá velar porque los funcionarios realicen las funciones propias de los cargos en condiciones ambientales favorables a fin de preservar la integridad del recurso humano.

Adicional deberá presentar informes con indicadores donde se refleje los conductos disciplinarios aplicados al personal por motivos donde se ve comprometida la seguridad de la información por último debe garantizar que todos los funcionarios de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón estén debidamente identificados por medio de un carnet de identificación que los acredite como miembros activos en calidad de empleados de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

Proveedores. Su función principal dentro del Sistema de Gestión de Seguridad de la Información será garantizar que los servicios contratados por la Curaduría Urbana No3 Arq. Ana María Cadena Tobón, en caso de tener alguna modificación ésta

deberá ser notificada al Asesor de sistemas con el propósito de validar las posibles afectación que ocasionan estos tipos de cambios, deben asistir a las reuniones programadas por el Asesor de sistemas en donde se socializarán temas en relación al Sistema de Gestión de Seguridad de la Información.

Usuarios. Deben estar comprometidos con el programa del Sistema de gestión de Seguridad de la Información cumpliendo a cabalidad las políticas establecidas, deben participar de las jornadas de sensibilización y su deber consiste en reportar al Administrador de Sistemas cualquier evento en donde se vea comprometida la seguridad de la información, deben de estar en la capacidad de dar el manejo adecuado a un evento de seguridad.

10.1.1.5 Comité de gestión de seguridad. El propósito de la creación de este comité tiene como fin apalancar el Sistema de Gestión de Seguridad de la Información, por este motivo su directriz apunta a hacer efectivo el cumplimiento de todo el SGSI de cara a la Curaduría Urbana No. 3 Arq. Ana María Cadena Tobón.

Este comité está conformado por el Director Administrativo, la Coordinación de Calidad, el Asesor de sistemas y los líderes de los procesos misionales. Quienes a su vez programaran reuniones mensuales para evaluar la efectividad del SGSI en aras de plantear una mejora continua, las temáticas a tratar en estos encuentros son relacionadas de la siguiente manera:

- Programar campañas informativas haciendo uso de diferentes estrategias comunicativas.

- Actualizar las políticas de Seguridad de la Información en caso de requerirse.

- Realizar la contratación de compañías externas consultoras en Seguridad de la Información para realizar la planeación de pruebas de Red Teams y Blue Teams

- Evaluar los Análisis recolectados en pruebas de gestión de incidentes a fin de socializar estrategias que permitan una mejora en el tratamiento de incidentes de seguridad de la información.

10.1.1.6 Propietarios de la información. Dentro del marco organizacional se delega como propietarios de la información a todos los líderes que hacen parte de los procesos misionales los cuales tienen a su cargo los activos de información en sus diferentes formas, es por este motivo, que sus responsabilidades apuntan a definir los criterios técnicos que se requieren con relación a la seguridad de la información.

Con base a los accesos que se deben tener según la matriz de roles y responsabilidades lo refleje, los propietarios de la información están en la capacidad

de evaluar qué información se clasifica como critica para darle el manejo adecuado en relación con el almacenaje, acceso por medio de privilegios y administración de activos fijos de información, lo anterior con el propósito de garantizar la seguridad de la información.

10.2 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA CURADURIA N. 3 ARQ. ANA MARIA CADENA TOBÓN

10.2.1 Política seguridad de los recursos humanos

Objetivo: establecer las políticas de seguridad con relación al recurso humano que hace parte de los procesos misionales en la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

Alcance: la directriz aplica al recurso humano que hace parte de los procesos misionales que hacen parte de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

Políticas

- Los funcionarios que hacen parte de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón deben estar contratados por medio de un contrato laboral en calidad de empleados.

- Los funcionarios que hacen parte de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, deben estar sujetos a una revisión de antecedentes como parte del proceso de contratación laboral.

- Los funcionarios que hacen parte de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón deben cumplir las responsabilidades e calidad de empleados y deben velar por el cumplimiento del Sistema de Gestión de Seguridad de la Información.

- Los funcionarios que hacen parte de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón deben participar activamente en las campañas de concienciación programadas como parte del Sistema de gestión de Seguridad de la Información.

- Los funcionarios que hacen parte de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, deben recibir un proceso de inducción e relación a las áreas que conforman los procesos misionales y estos a su vez están en la obligación de adherirse al cumplimiento de las políticas de seguridad.

- Los funcionarios que hacen parte de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón deben reportar al líder del área las novedades que comprometan la

seguridad de la información.

- El incumplimiento de las políticas de seguridad de la información está sujeto a sanciones disciplinarias.

- Al finalizar el contrato laboral celebrado entre el empleador y el empleado es responsabilidad del usuario entregar los activos físicos de información en el estado en que fuesen asignados.

- Es obligación de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón en apoyo con la ARL desarrollar jornadas de pausas activas a los funcionarios que hacen parte de los procesos misionales.

- Los contratos laborales deben están sujetos a la inserción de una cláusula de confidencialidad para aplicar al recurso humano en calidad de empleados de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

- Es deber de los funcionarios portar el carné de identificación que los hace miembros activos de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón durante la permeancia en las instalaciones de la institución.

- Los funcionarios de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón deben tomar una posición de responsabilidad directa en el Sistema de gestión de Seguridad de la Información.

- Los funcionarios que hacen parte de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón deben conocer las matrices de roles y responsabilidades socializada por el área de calidad durante el proceso de inducción.

10.2.2 Política de gestión de activos

Objetivo: establecer las políticas de seguridad a tener en cuenta en relación a la gestión de activos con el propósito de proteger los activos de información en la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón

Alcance: la directriz aplica a todos el recurso humano que hace parte de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

Política

- Los activos físicos de información deben estar correctamente identificados por medio de una placa metálica que contenga el nombre de la institución tipo de activo y serial.

- Los activos físicos de información deben estar relacionados por medio de un inventario en un sistema que permita acceder a una consulta actualizada para su disposición.

- Los líderes de área deben tener total claridad de que activos de asignan a los usuarios con el propósito de establecer un marco de responsabilidad.

- Cuando se termina el vínculo laborar entre el empleador y el empleado es responsabilidad del empleado entregar los dispositivos de información asignados en las mismas condiciones recibidas con el propósito de reasignarlo para fines pertinentes.

- La información física como documentos licencias y demás actuaciones debe estar previamente identificadas y organizadas en archivadores con fin de preservar la integridad de estas.

- Los activos de información asignados a los funcionarios como computadores impresores y celulares corporativos son única y exclusivamente para el ejercicio propio de las labores de los cargos y su uso no debe remitirse a fines personales, de hacerse y comprobarse se deberá aplicarse el conducto regular disciplinario.

- Al interior de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón no se deben utilizar dispositivos de almacenamiento extraíble como discos duros, memorias USB entre otros medios ópticos, cuando no son de propiedad de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón, de utilizarse estos deben estar previamente autorizados por el jefe del Área y Asesor de Sistemas.

- El administrador de sistemas se encargará de realizar las copias de seguridad de los medios de información granizando el uso de medios de cifrado que permitan garantizar la confidencialidad.

- Las copias de seguridad físicas se alojarán en un recinto que cuente con las condiciones ambientales favorables con relación a humedad, fuego, polvo.

- Cuando los usuarios terminen su contrato laboral en calidad de empleados con la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón se deberá realizar un backups local del activo de información asignado (computador) y de la unidad de red asignada, copia que se alojara en un recinto seguro.

10.2.3 Política de control de acceso

Objetivo: establecer las políticas de control a tener en cuenta al momento de acceder a la información dentro de los procesos misionales en la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

Alcance: la directriz aplica a todos el recurso humano que hace parte de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón en calidad de empleados sustentado por medio de contrato laboral.

Política

- Una vez el proceso contractual de contratación a empleados está debidamente legalizado, el administrador de sistemas creará los usuarios pertinentes en los sistemas informáticos y realizará la entrega de credenciales mediante acta de socialización con firma en común acuerdo entre el empleado y la Curaduría Urbana representada por el administrador de sistemas.

- Las credenciales de acceso a los sistemas de información serán generadas por defecto con la propiedad de ser cambiadas por el usuario en el primer logueo garantizando la confidencialidad.

- Los criterios de contraseñas deberán contener caracteres en mayúsculas, caracteres en minúsculas una base de 10 dígitos y un carácter espacial.

- Las contraseñas deber ser personales e intransferibles y estas o se deben compartir en ninguna circunstancia sin previa autorización por parte del líder de áreas.

- En lo posible se debe garantizar que el acceso a los sistemas informáticos por medio de la administración se realice de manera sincronizada haciendo uso de credenciales de Directorio Activo.

- Las cuentas de usuarios que no presenten una actividad en un periodo de tiempo de 60 días se deben deshabilitar.

- Se debe configurar una gestión de claves para caducidad con relación de tiempo de 30 días, tiempo en el que el usuario deberá actualizar su credencial.

- Cuando un usuario finalice el contrato laboral con la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón se deberá utilizar el documento de ruta Paz y salvo en donde este debe contener la firma y sello de los líderes de área siento el administrador de sistemas el último en firmar la hoja de tal modo que se reciba el equipo asignado he inmediatamente se realice la desactivación de lo usuario en los sistemas de información.

- Al momento de ingresar a instalaciones donde se encuentran el data center, unidades de procesamiento y almacenamiento, se debe registrar la persona o proveedor por medio de una bitácora justificando el motivo, hora de ingreso y hora de salida, este ingreso debe estar autorizado por el Asesor de Sistemas.

- La creación de VPN para utilizar de manera remota deberá ser autorizada por el Líder de área justificando el motivo de tal creación, y esta solo se podrá utilizar en os equipos que hacen parte del inventario de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón no en equipos personales.

- La información que parte de los procesos misionales se debe guardar en las unidades de red autorizadas por el Asesor de sistemas, el Dpto. de Tecnología no se hará responsable por información que por algún motivo se pueda perder y que se encuentre en otra ubicación distinta.

- La Dirección Administrativa y líderes de área tendrán la responsabilidad de autorizar los permisos los cuales tendrán los usuarios al momento de acceder a la información.

- No deben existir más de una cuenta creada en los sistemas de información a nombre de un solo usuario.

- Se debe tener una cuenta de red disponible para acceder a los sistemas de información con privilegios mínimos con el propósito de ser utilizada cuando se requiera utilizar por proveedores en ciertos momentos específicos.

10.2.4 Política de seguridad física y del entorno

Objetivo: establecer las políticas a tener en cuenta en relaciona la seguridad física y del entorno al con el propósito de garantizar la seguridad de la información e la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

Alcance: la directriz aplica a todos el recurso humano que hace parte de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

Política

- La Curaduría Urbana N.3 Arq. Ana María Cadena Tobón debe contar con sistemas de monitoreo interno como alarmas de intrusos físicos y sistemas de fuegos para contrarrestar desastres naturales.

- Los funcionarios que hacen parte de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón deberán permanecer debidamente identificados por medio de carné corporativo que los acredita como funcionarios activos de la institución.

- Se debe revisar y actualizar la matriz de riesgos y un periodo trimestral y a su vez esta debe ser socializada con los funcionarios de la institución.

- Los activos físicos de información deben estar ubicados en lugares donde se

preserve su integridad y se protejan contra eventos físicos garantizando de este modo la continuidad operacional.

- Los equipos con carga alta de operación como servidores y unidades de almacenamiento, computadores deben contar con sistemas alternos de flujo de corriente eléctrica regulada.

- Los puntos de red internos deben ser previamente certificados por entidades que garanticen los estándares del mercado cumpliendo la normatividad actual.

- La información física manejada en los procesos misionales debe estar salvaguardada en un recinto en condiciones libres de humedad, polvo, y con acceso único al personal autorizado para el ejercicio propio de las funciones de los cargos.

- Se debe dar cumplimiento al cronograma de mantenimiento de equipos de cómputo anualmente según programación planteada por el Asesor de Sistemas en los tiempos estimados.

- Al retirarse un equipo de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón con fines laborales este debe contar con una póliza que tenga una cobertura por robo perdida o daño.

- Ates de retirar los equipos de la institución, es usuario deberá asegurarse que estos se encuentras en óptimas condiciones funcionales y operacionales.

- Por ningún motivo se debe consumir alimentos en las estaciones de trabajo en donde se encuentren equipos electrónicos como computadores, medios de almacenamiento externos, unidades removibles entre otros periféricos que se puedan ver sometidos a daños.

- Cada activo físico de información como computadores de escritorio, portátiles, servidores y demás dispositivos de comunicación deben contar con guayas de seguridad de alta calidad.

- Se debe implementar en conjunto con las unidades de atención a emergencias un protocolo en caso de presentarse un evento o desastre naturales en donde se vea comprometida los activos de información.

- Se deben contar con sistemas biométricos de acceso a las instalaciones de la institución con el propósito de llevar un control del personal circundante.

10.2.5 Políticas de seguridad de la operación del negocio

Objetivo: establecer las políticas de seguridad que permitan garantizar la operación y continuidad del negocio

Alcance: la directriz aplica a todo el recurso humano y proveedores que ofertan servicios a los procesos misionales en la Curaduría Urbana N.3 Arq. Ana maría Cadena Tobón.

Política

- La Dirección Administrativa debe estar comprometida con la socialización de los procesos internos de cara a los funcionarios y proveedores de servicios de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

- La adquisición de software adicional para el ejercicio propio de los cargos debe ingresar en un proceso de consultoría por parte del Asesor de sistemas y posteriormente debe estar aprobada por parte de la Dirección Administrativa.

- Los equipos deben contar con una imagen que contenga todo el software que se utilizara en las maquinas que los funcionarios a fin de garantizar que no se instale software que no ha sido autorizado para su uso.

- El software instalado en las máquinas debe ser registrado por medio de una lista de chuqueo la cual se aplicará al momento de realizar jornadas de Mtto de equipos.

- El Administrador de sistemas será la única persona autorizada para realizar las instalaciones de periféricos adicionales y software en general.

- Todo el software utilizado en la Curaduría Urbana No.3 debe contar con las respectivas licencias y estas deben estar consignadas en un documento relacionadas con el serial del equipo donde se encuentra instaladas para efectos de auditorías.

- El uso de Software libre debe estar justificado para su uso y este debe estar avalado por parte del Asesor de Sistemas y aprobado por la Dirección Administrativa.

- Los proveedores que suplen de algún servicio a la Curaduría urbana No. 3 Arq. Ana María Cadena Tobón deben integrarse en las actividades de concienciación como parte fundamentar en el Sistema de Gestión de Seguridad de la Información.

- Los proveedores que suplen de servicios a la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón deberán elaborar planes de contingencia que permitan

garantizar la continuidad del negocio en un evento donde se comprometa la seguridad de la información.

- Las firmas digitales y Hash catalogados como maliciosos deben actualizarse inmediatamente haciendo uso de un procedimiento en el motor de antivirus para garantizar la seguridad de la información.

- En relación con las copias de las bases de datos, estas deben estar sujetas a un proceso de auditoria por parte del Asesor de sistemas con el propósito de garantizar que la información se encuentra correctamente respaldada, este proceso se debe realizar de manera semanal.

- Todos los equipos de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón deberán estar sincronizados en relación con la zona horaria y hora, para ello es importante definir un único servidor (Network Time Protocolo) quien garantizara la efectividad de este ciclo horario.

- Los eventos de seguridad reportados por parte de los usuarios deben tener un seguimiento riguroso por parte del administrador de sistemas con el propósito de elaborar una base de conocimiento y lección aprendía para futuras situaciones en donde se comprometa la seguridad de la información.

- Los eventos en donde se comprometa la seguridad de la información deberán ser tratados en el comité de Gestión de Seguridad, con el propósito de ser socializados e indagados previamente.

- La Dirección Administrativa deberá garantizar un equipo de respaldo (switch, servidor, AP, Modem) para ser utilizado en caso de presentarse un evento en donde por algún motivo se frene la operación, este debe contar con configuraciones base realizadas por medio del Administrador de Sistemas.

- Los eventos identificados deben ser actualizados en la matriz de riesgos y esta deberá ser presentada en el comité de Gestión de Seguridad de la Información a fin de poner en contexto a la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

10.2.6 Política de seguridad de las comunicaciones

Objetivo: establecer las políticas de seguridad que permitan garantizar la seguridad de la información en relación con la red de comunicaciones

Alcance: la directriz aplica para los usuarios, líderes de área, Asesor de sistemas, administrados de Sistemas y proveedores.
Política

- La Dirección Administrativa deberá garantizar una estación de trabajo a cada funcionario de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón que se encuentre en calidad de empleado sujeto a contrato laboral, el cual debe contar con un computador y conexión a internet para el ejercicio de las funciones propias del cargo.

- Se restringe la navegación a internet para sitios como redes sociales, tiendas online, y ubicaciones de consulta que no se adhieran a las funciones propias de los cargos organizacionales.

- La navegación abierta debe ser aprobada por el Director Administrativo y utilizada únicamente por los líderes de área para el ejercicio de las funciones.

- Los equipos de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón deberán contar con un sistema de protección por medio de un UTM o Firewall, allí no se podrá realizar la conexión de equipos personales sin previa autorización del director administrativo y Asesor de Sistemas.

- Se debe contar con una contingencia en alta disponibilidad en canales de Internet para caso de caída del servicio, por tal motivo el UTM deberá contar con estos recursos previamente configurados.

- Se debe contar con un contrato legal firmado para recibir soporte sobre dispositivos de comunicación como (SWITCH, UTM, AP,).

- El proveedor debe garantizar en común acuerdo con el Asesor de Sistemas la elaboración y presentación de planes de trabajo para la ejecución de jornadas de mantenimiento a dispositivos de comunicación.

- Se restringe el uso de correo personales para él envió y recepción de información laboral.

- Todos los correos corporativos deberán contener una firma digital donde se muestra claramente el remitente de tal correo.

- Los contratos que se celebren entre la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón y los proveedores, deben tener un acuerdo de confidencialidad gratinando la seguridad de la información.

- Se debe registrar los eventos de seguridad reportados ocasionados por el proveedor de servicios y socializados en comité de gestión de seguridad.

- Se deben programar pruebas de Red Teams y Blue Teams en periodos de tiempos programados con el asesor de sistemas.

- Se deben aplicar planes de remediación teniendo como base los resultados arrojados por el equipo de Red Teams y Blue Teams.

10.2.7 Políticas de seguridad con proveedores

Objetivo: establecer las políticas de seguridad con proveedores garantizando la seguridad de la información.

Alcance: las políticas de seguridad aplican para proveedores que suplan a la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón de servicios.

Políticas

- Los contratos celebrados entre la Curaduría Urbana N.3 Arq. Ana María cadena Tobón y proveedores de servicios deben estar sujetos al cumplimiento de los servicios contratados por medio de ANS o tiempos especificados.

- De incumplirse los ANS pactados, estos están sujetos a la aplicación de cláusulas económicas.

- Los contratos celebrados entre la Curaduría Urbana N.3 Arq. Ana María cadena Tobón deben estar sujetos al cumplimiento de cláusulas de confidencialidad, el no cumplimiento ocasionara de manera inmediata la cancelación de los servicios contratados.

- Es responsabilidad de los proveedores de servicios adherirse a las políticas de sistemas de gestión de seguridad de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón.

- Los proveedores de servicios deben contar con planes de externos en la prestación de los servicios en donde se garantice la continuidad del negocio por efectos en donde se comprometa la seguridad de la información.

- Los proveedores de servicios deben asistir a las reuniones programadas por parte de Asesor de sistemas con el propósito de auditar el cumplimiento de los servicios contratados.

- La no adhesión al sistema de gestión de seguridad de la información incurrirá en la terminación contractual de los servicios contratados.

- La Curaduría Urbana No.3 Arq. Ana María Cadena Tobón realizara oportunamente el pago de los servicios contratados según facturación radicada en las fechas estimadas

11. PLAN DE CONCIENCIACIÓN

11.1 GENERALIZACIÓN

Tomando como referencia el framework NIST 800-50 orientado al desarrollo de un plan de concienciación, es importante tener en cuenta que:

> No se puede implementar un programa de seguridad de TI sólido sin una atención significativa a la capacitación de los usuarios de TI de la agencia sobre políticas, procedimientos y técnicas de seguridad, así como los diversos controles administrativos, operativos y técnicos necesarios y disponibles para asegurar los recursos de TI. Además, aquellos en la agencia que administran la infraestructura de TI deben tener las habilidades necesarias para llevar a cabo sus tareas asignadas de manera efectiva. No prestar atención al área de capacitación en seguridad pone a la empresa en un gran riesgo porque la seguridad de los recursos de la agencia es tanto un problema [48]

Dentro de las características principales que se mencionan en un plan de concienciación propuesto en el framenwork de la NIST 800-50 hace referencia a que este debe contener conciencia, educación y entrenamiento siendo estos elementos esenciales al momento de buscar una mantención en el tiempo.

11.1.1 Conciencia.

> La conciencia es el esfuerzo de concienciación sobre seguridad están diseñados para cambiar el comportamiento o reforzar las buenas prácticas de seguridad. La conciencia no es entrenamiento. El propósito de las presentaciones de sensibilización es simplemente centrar la atención en la seguridad. Las presentaciones de sensibilización están destinadas a permitir que las personas reconozcan las preocupaciones de seguridad de TI y respondan en consecuencia.[49]

Cuando se tiene conciencia existe un cambio de cultura y es allí donde se da valor a la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

11.1.2 Entrenamiento. El entrenamiento se define según la NIST 800-16 como:

> El nivel de 'Capacitación' del continuo de aprendizaje se esfuerza por producir habilidades y competencias de seguridad relevantes y necesarias por parte de profesionales de especialidades funcionales distintas de la seguridad de TI
>
> La diferencia más significativa entre la formación y la conciencia es que la

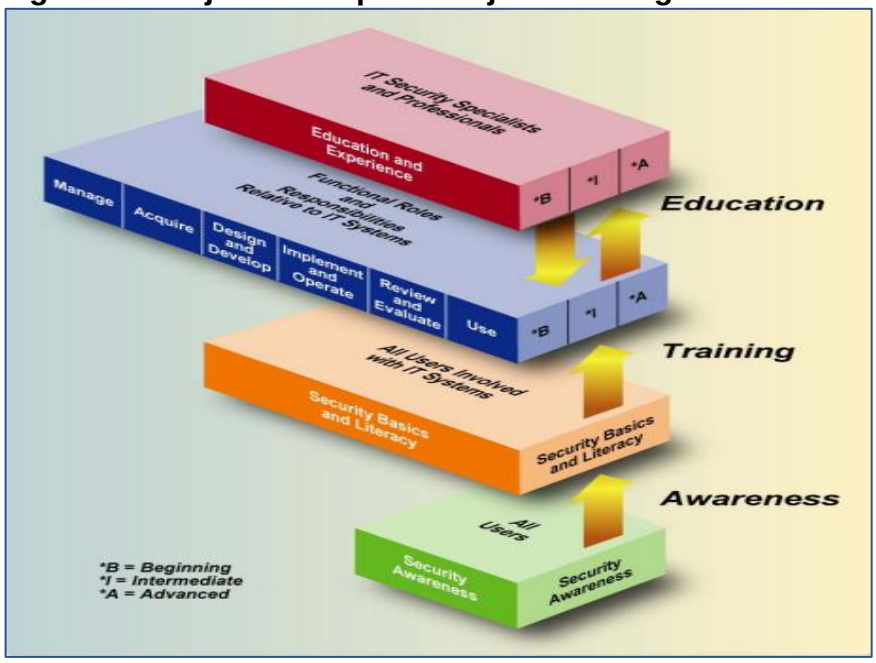
[48] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Computersecurity. 800-50. Gaithersburg. EE. UU, 2003.p.23.
[49] Ibid., p.44

formación busca enseñar habilidades, que permiten a una persona realizar una función específica, mientras que la conciencia busca centrar la atención de un individuo en un tema o conjunto de problemas. Las habilidades adquiridas durante la capacitación se basan en la base de la conciencia, en particular, en los conceptos básicos de seguridad y el material de alfabetización[50]

Por lo anterior es importante que se exista una correlación con el propósito de adquirir habilidades necesarias y adheridas en el día a día o en el ejercicio de las funciones propias de los cargos en la Curaduría Urbana No3 Arq. Ana María cadena Tobón.

11.1.3 Educación. La educación es definida como aquel ente que "integra todas las habilidades y competencias de seguridad de las diversas especialidades funcionales en un cuerpo común de conocimiento, agrega un estudio multidisciplinario de conceptos, problemas y principios (tecnológicos y sociales) y se esfuerza por producir especialistas en seguridad de TI y profesionales capaces de visión y respuesta proactiva"[51]. El contexto cotidiano permite a los funcionarios de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón poner en práctica y adquirir tanto el conocimiento como la practica en un contexto real. En la presente imagen se evidencia como está conformado un plan de concienciación apalancado en el frameword de la NIST 800-50. (ver figura 6 y 7)

Figura 6. Conjunto de aprendizaje sobre seguridad TI.



Fuente: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Computersecurity. 800-50. Gaithersburg. EE. UU, 2003.p.33.

[50] Ibid.,p.49.
[51] Ibid.,p.49.

Figura 7. Modelo de gestión de programa centralizada

Fuente: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Computersecurity. 800-50. Gaithersburg. EE. UU, 2003.p.33.

Este modelo se caracteriza dado a que la "responsabilidad y el presupuesto del programa de capacitación y concienciación sobre seguridad de TI de toda la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón se otorga a una autoridad central. Todas las directivas, el desarrollo de estrategias, la planificación y la programación se coordinan a través de esta autoridad de "concienciación y capacitación en seguridad"[52], dentro de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón inicia este tipo de iniciativa desde el Dpto. de Tecnología.

Por lo anterior el modelo a tomar como base para la construcción del plan de concienciación es el modelo de programa centralizado.

Las estrategias comunicativas de cara a los usuarios buscan crear cultura que genere un cambio organizacional, por tal motivo es importante hacer uso de estrategias comunicativas con el propósito de socializar el sistema de gestión de seguridad de la información. Actualmente en la curaduría urbana No. 3 Arq. Ana María Cadena Tobón no se cuenta con esta cultura por parte de los usuarios lo que ocasiona que se generen incidentes de seguridad y se vulnere los activos de información que conforman los procesos misionales.

Las actividades propuestas que a continuación se mencionan e involucran a todos los componentes que hacen parte de los procesos misionales, con el apoyo de la

[52] Ibid.,p.29.

Dirección Administrativa, lo que busca es mantener este tipo de estrategias comunicativas vigentes para que se propaguen en todo el tiempo de tal modo que periódicamente se realice un análisis para visualizar el cambio de cultura organizacional por parte de los usuarios y a su vez validar las mejores prácticas que los usuarios adhieren al ejercicio de las funciones propias de los cargos laborales.

11.2 OBJETIVO

- Crear conciencia en los usuarios que hacen parte de los procesos misionales en la curaduría urbana No.3 Arq. Ana María Cadena Tobón, mostrando la importancia de cada uno de ellos en relación con al sistema de gestión de Seguridad de la información.

- Socializar el Sistema de Gestión de Seguridad de la Información a los proveedores o terceros que suplen de algún servicio a la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón, de tal modo que se cree conciencia en ellos como parte fundamental en los objetivos de negocio.

- Socializar a los usuarios y proveedores que hacen parte de los procesos Misionales de la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón los riesgos, amenazas a los que en la cotidianidad se encuentra expuesta los activos de información y como estos impactan los objetivos de negocio.

- Generar un cambio de cultura organizacional para que se mantenga en el tiempo.

- Socializar las políticas de seguridad de la información definidas y aprobadas por la Gerencia con base en la norma ISO/IEC 27001:2013.

11.3 ALCANCE

El plan de concienciación tiene un alcance general en los que abarca los componentes o recursos humanos que hacen parte de los procesos misionales, los cuales se mencionan a continuación:

Gerencia General: Líderes de los procesos misionales (emisión de conceptos, radicación, estudios técnicos, expedición entrega y notificación de licenciamiento urbanístico). Empleados que hacen parte de los procesos misionales.

Proveedores de servicio: Los cuales suplen a la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón en relación con los servicios contratados.

11.4 ESTRATEGIA

Con el propósito de socializar a los usuarios que hacen parte de los procesos

misionales en la curaduría urbana No.3 Arq. Ana María Cadena Tobón, se estableció un plan de trabajo que está compuesto con las siguientes estrategias que buscan poner en contexto, formar a los usuarios y adherir las mejores prácticas en seguridad de la información; con base en lo anterior, los recursos a poner en marcha se mencionan a continuación:

- Socialización por medio de reuniones.
- Capacitaciones a usuarios con temáticas definidas.
- Elaboración de campaña visual para los usuarios.
- Entrega de información útil de bolsillo.
- Envió de correos masivos socializando políticas.
- Evaluaciones elaboradas por medio de formularios elaborados.

11.4.1 Desarrollo en escenario

11.4.1.1 Socialización por medio de reuniones. La socialización por medio de reuniones es la primera estrategia utilizada para realizar un primer acercamiento a los usuarios con el propósito de dar a conocer la Norma ISO/IEC 27001:2013 a nivel general, de tal modo que por medio de 1 encuentro semanal se ponga en contexto sobre las ventajas de adherir un Sistema de Gestión de Seguridad de la Información a los procesos organizacionales. En este caso particular misionales, como evidencia se llevará registro de asistencia por medio de un formato codificado por la Coordinadora integrada de sistema de Gestión (SIG) con el propósito de llevar una estadística de participación de usuarios que reciben la socialización para fines pertinentes. (Ver Anexo C registro acta de reunión).

11.4.1.2 Capacitaciones a usuarios con temáticas definidas. Como segunda estrategia se proyectó un cronograma de capacitaciones a realizar en el primer semestre de 2021, las temáticas relacionadas involucran los actores que hacen parte de los procesos misionales (Ver cuadro 16).

Cuadro 16. Cronograma de capacitaciones

Tema	Objetivo	Dirigido	Desarrollo	Recurso	Fecha	Evidencia
Que es un SGSI	Socializar a los funcionarios sobre que es un Sistema de Gestión de Seguridad de la Información.	Funcionarios que hacen parte de los procesos misionales	Por medio de reuniones se pondrá en contexto a los funcionarios de la institución la definición, componentes se SGS	Presentación en Power Point	• Febrero 02-2021 • Febrero 08-2021	Registro de asistencia codificado por el Dpto. de Calidad
Riesgos a los que se expone los activos de información	Concientizar a los usuarios que hacen parte de los procesos misionales sobre los riesgos a los que están expuestos los activos de información.	Funcionarios que hacen parte de los procesos misionales	Por medio talleres lúdicos sensibilizar a los usuarios sobre los riesgos que se desarrollan en un ambiente laboral	Casos de análisis reales	• Febrero 15-2021	Registro de asistencia codificado por el Dpto. de Calidad
Reacción ante eventos de seguridad	Orientar a los usuarios sobre cómo actuar ante un posible evento que la seguridad de la información dentro de la organización.	Funcionarios que hacen parte de los procesos misionales	Por medio un video lúdico ilustrar a los usuarios sobre cómo reaccionar y que acciones tomar cuando se compromete la seguridad de la información	Proyección de videos	• Febrero 22-2021	Registro de asistencia codificado por el Dpto. de Calidad
Socialización de políticas de seguridad de la información	Socializar a los funcionarios de la institución las políticas aprobadas por la Gerencia para poner en uso.	Funcionarios que hacen parte de los procesos misionales	Se realizará la entrega de Brochur socializando las políticas de seguridad de la información a título informativo a los usuarios.	Brochur informativo	• Marzo 01-2021	Registro de asistencia codificado por el Dpto. de Calidad con nota de entrega de material informativo

Cuadro 16. (Continuación)

Tema	Objetivo	Dirigido	Desarrollo	Recurso	Fecha	Evidencia
Prestación continua de servicios adquiridos de TI	Involucrar a los proveedores como parte fundamental en el sistema de gestión de seguridad de la información.	Proveedores y prestadores de servicios TI	Reuniones donde participe la Gerencia, el Dpto. de Calidad, Dpto. de TIC y los proveedores	Auditorio Presentación Power point	• Marzo 08-2021 • Marzo 15-2021 • Marzo 29-2021	Registro de asistencia codificado por el Dpto. de Calidad
Continuidad de negocio Primera parte	Orientar a la alta Gerencia, Dpto. de Calidad, y Dpto. TIC sobre estrategias para la recuperación de desastres y continuidad de negocio.	Gerencia, Dpto. Calidad, Dpto. TIC	Reuniones donde participe la Gerencia, el Dpto. de Calidad, Dpto. de TIC en acompañamiento comuna entidad consultora en seguridad de la información	Auditorio Presentación Power point	• Febrero 05-2021 • Febrero 26-2021 • Marzo 05-2021 • Marzo 26-2021	Registro de asistencia codificado por el Dpto. de Calidad
Continuidad de negocio Segunda Parte	Orientar a la alta Gerencia, Dpto., de Calidad, y Dpto. TIC sobre estrategias para la recuperación de desastres y continuidad de negocio.	Gerencia, Dpto. Calidad, Dpto. TIC	Reuniones donde participe la Gerencia, el Dpto. de Calidad, Dpto. de TIC en acompañamiento comuna entidad consultora en seguridad de la información	Auditorio Presentación Power point	• Abril 05-2021 • Abril 26-2021 • Mayo 03-2021 • Mayo31-2021	Registro de asistencia codificado por el Dpto. de Calidad
Evaluación y tratamiento de riesgos	Conocer, validar y gestionar las estrategias para realizar el tratamiento de riesgos de manera adecuada como mejora continua.	Gerencia, Dpto. Calidad, Dpto. TIC	Reunión con una entidad tercerizada experta en consultoría en seguridad de la información	Auditorio Presentación Power point	• Junio 04-2021 • Junio 11-2021 • Junio 18-2021 • Junio 25-2021	Registro de asistencia codificado por el Dpto. de Calidad
Evaluación del programa de capacitación Reprogramación de temario para segundo semestre de año 2021						

Fuente. Los Autores

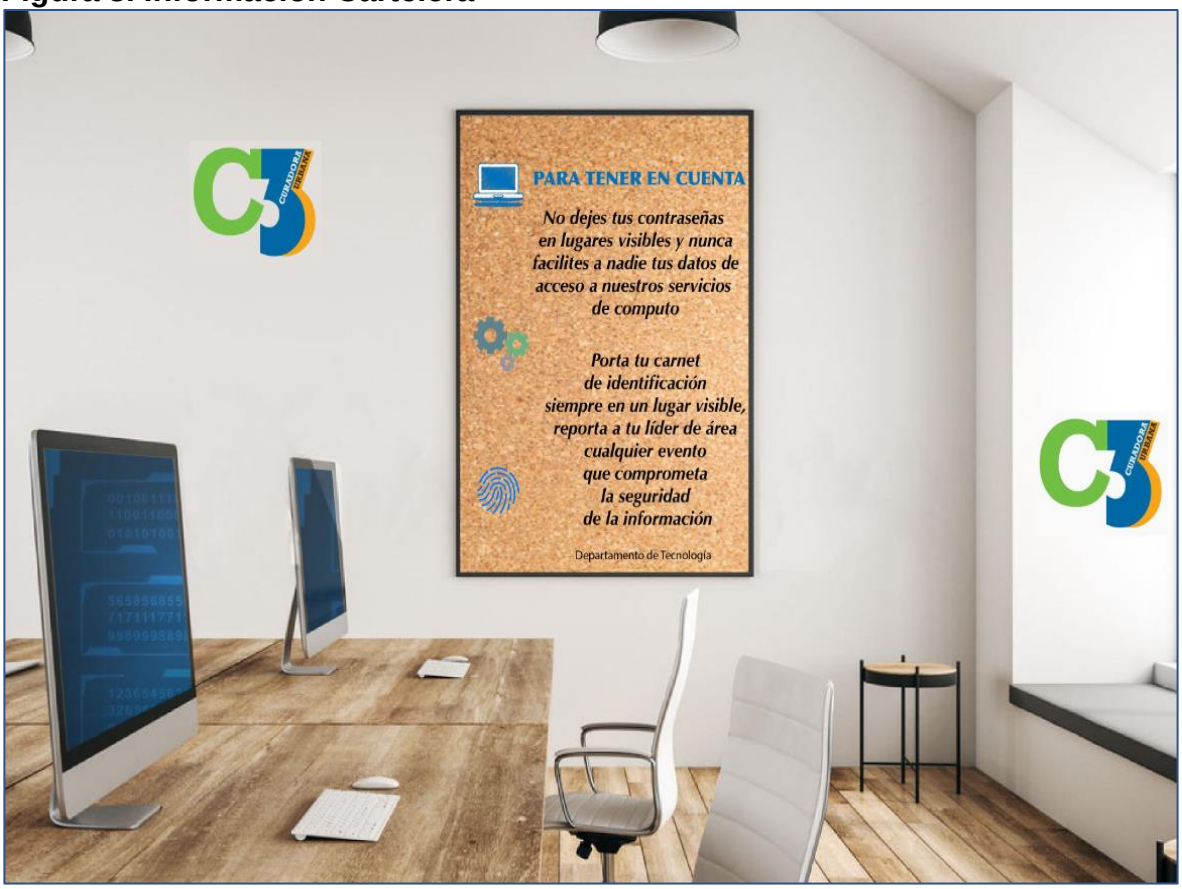
11.4.1.3 Elaboración de campaña visual para los usuarios. Con el propósito de apoyar la socialización a los usuarios con relación al Sistema de Gestión de Seguridad de la Información, se identificaron los puntos claves que sirven como factor primario para la divulgación de información útil, estos espacios están divididos del siguiente modo

- Carteleras corporativas.
- Fondos de pantalla en los pc de la institución.
- Información publicada en la página Web.

La información impresa y publicada está sujeta a cambios para poder mantenerla en el tiempo de tal modo que genere impacto y no sea tediosa.

Ejemplo cartelera y fondo de pantalla (ver figura 8 y 9)

Figura 8. Información Cartelera



Fuente. Los Autores

Figura 9. Fondos de pantalla seguridad de la información

Fuente. Los Autores

11.4.1.4 Entrega de información útil de bolsillo. Una de las estrategias que más genera impacto en los usuarios es la creación de volantes que permitan socializar tips útiles en relación con las mejores prácticas que se deben adoptar para la creación de conciencia y el cambio de cultura organizacional, la entrega de volantes se realizara de manera paulatina y toda vez que se realice las capacitaciones a usuarios. ejemplo (ver figura 10,11 y 12)

Figura 10. Catálogos sobre seguridad informática 1.

Fuente: Los autores

Figura 11. Catálogos sobre seguridad informática 2.

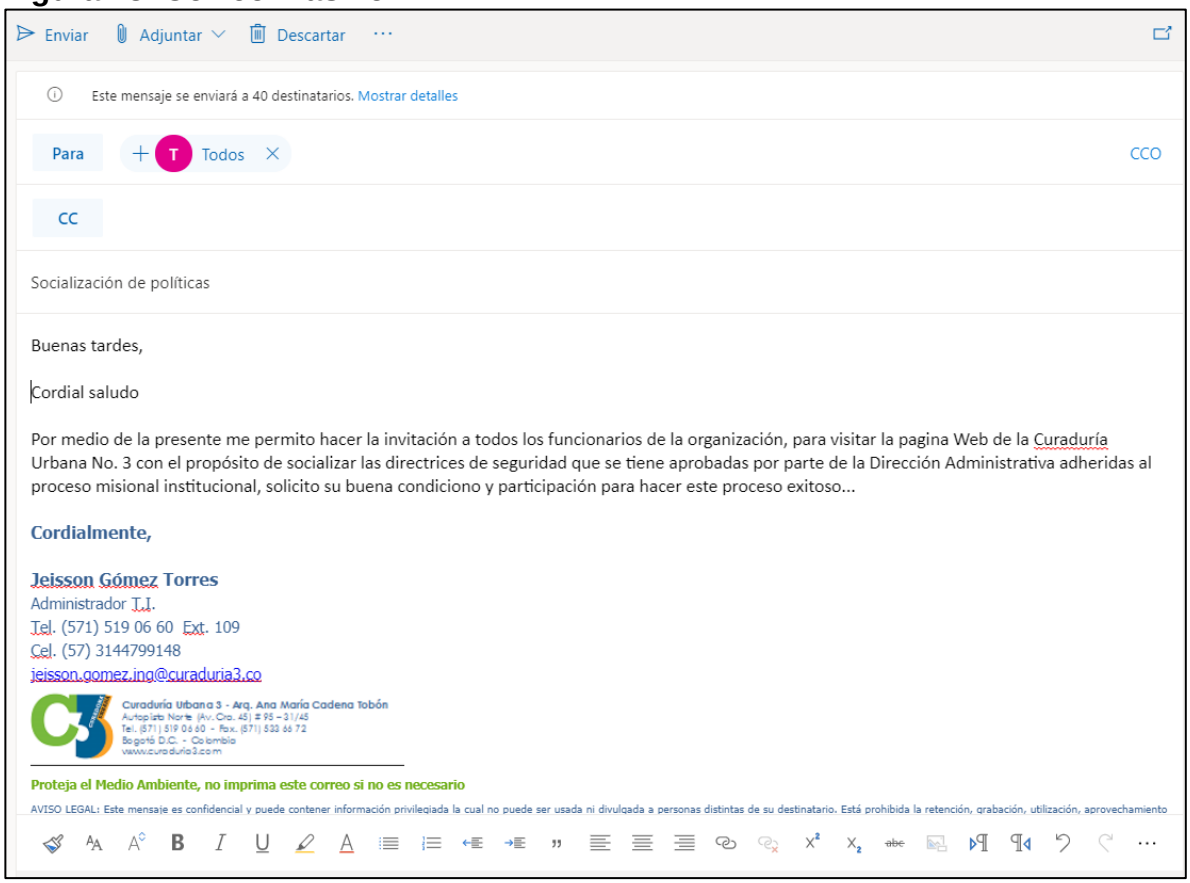
Fuente: Los autores

Figura 12. Catálogos sobre seguridad informática 3.

Fuente: Los autores

11.4.1.5 Envió de correos masivos socializando las políticas. Se realizará él envió de varios correos masivos socializando las políticas que fueron aprobadas por la Gerencia con el propósito de reforzar la divulgación de estas directrices para su cumplimiento obligatorio. (ver figura 13)

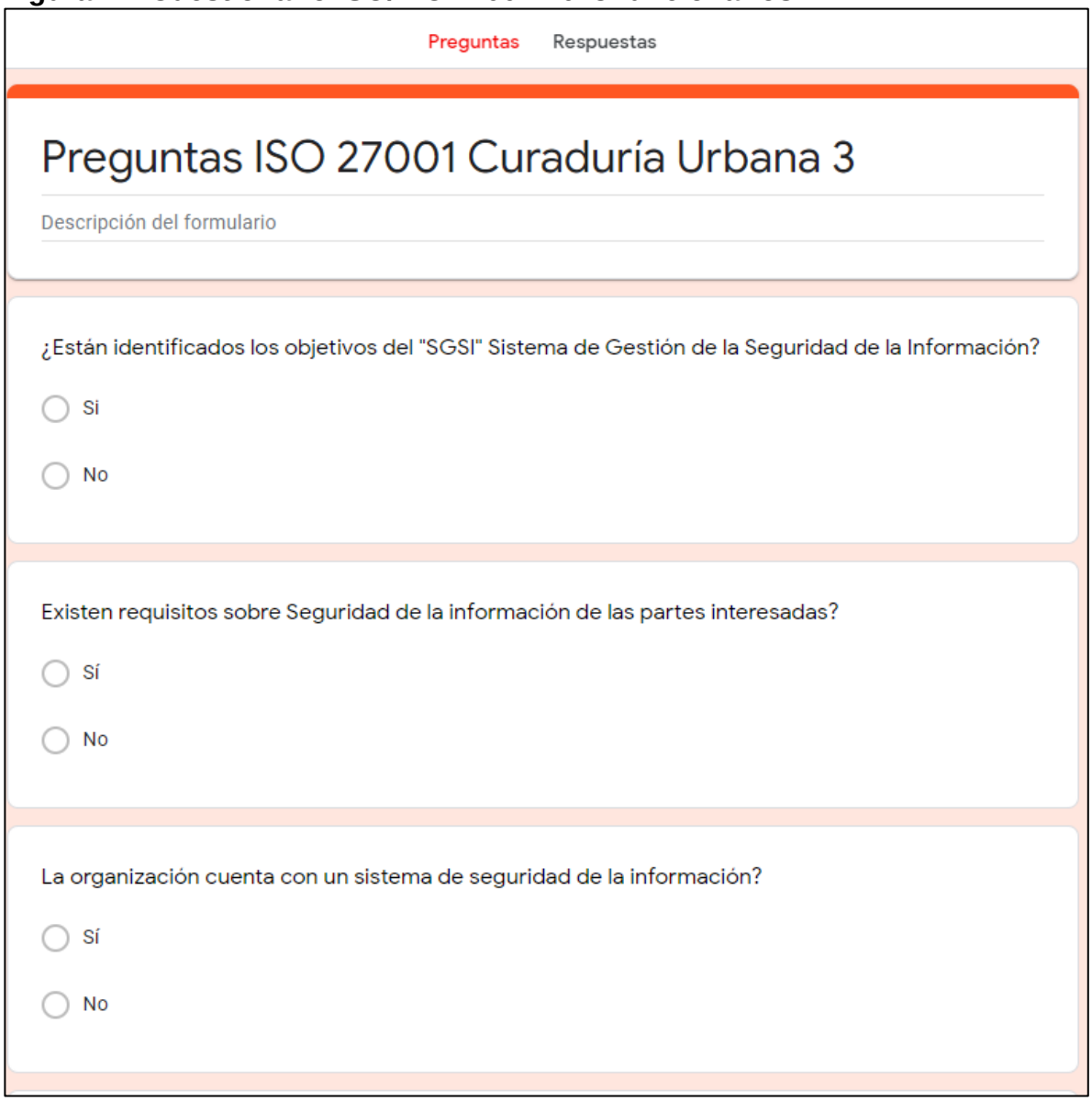
Figura 13. Correo masivo



Fuente. Los autores

11.4.1.6 Evaluaciones elaboradas por medio de formularios. Cantidad de los mecanismos más acertados para validar que tanto los funcionarios de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón están familiarizados con el Sistema de Gestión de Seguridad de la Información va orientado en la realización de evaluaciones periódicas con el propósito obtener tener una medición que permita reforzar los temas que por algún motivo no han tenido la suficiente claridad, de este modo lo que se quiere es replantear las estrategias de comunicación que se utilizaran al momento de divulgar la temática trasmitida, estas evaluaciones serán realizadas por medio de formularios elaborados y cargados por medio de la herramienta Google Forms y la temática relacionada será avalada por el Dpto. de Calidad. (ver figura 14)

Figura 14. Cuestionario ISO/IEC 27001:2013 funcionarios.



Preguntas Respuestas

Preguntas ISO 27001 Curaduría Urbana 3

Descripción del formulario

¿Están identificados los objetivos del "SGSI" Sistema de Gestión de la Seguridad de la Información?

- Si
- No

Existen requisitos sobre Seguridad de la información de las partes interesadas?

- Sí
- No

La organización cuenta con un sistema de seguridad de la información?

- Sí
- No

Fuente. Los autores

12. CONCLUSIONES

La propuesta para la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón cuyo objeto de estudio refiere al diseño de un Sistema de Gestión de Seguridad de la Información, para los procesos misionales de licenciamiento, concluye que atendiendo a los objetivos planteados:

- En cuanto al estado actual de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón y en correspondencia con los resultados obtenidos tanto en el cuestionario ISO/IEC 27001:2013 aplicado a la alta Gerencia y la encuesta aplicada a los funcionarios de los procesos misionales; se establece que no existe una claridad en relación a la definición de SGSI, componentes y su rol dentro del mismo, no se cuenta con una contextualización en relación a los riesgos presentes a nivel de Seguridad de la información y como estos se tratan, se carece de capacitaciones, del mismo modo la alta Gerencia presenta un avance significativo en relación al cumplimiento de algunos dominios y controles de la Norma 27001:2013 /IEC: 2013 los cuales requieren ser revisados y afinados a fin de garantizar la seguridad de la información, anqué se cuenten con mecanismos de protección a nivel de infraestructura , estos requieren ser apalancados por medio de procedimientos definidos.

- Al realizar un análisis al interior de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón se evidencio que no se tenía un conocimiento en relación a la definición de un Sistema de Gestión de Seguridad de la Información por parte de la Dirección Administrativa, Coordinación Integrada del Sistema de Gestión ni de los usuarios que conforman los procesos misionales en la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, aunque para algunos de ellos les eran conocido el concepto de SGSI.

- Respecto a la clasificación de los activos de información que hacen parte de los procesos misionales se logró realizar una identificación de activos, lo que conllevo a generar un inventario general que establece un orden estandarizado en nomenclatura y tipo. lo anterior permitió tener un panorama claro en relación a que activos de información tienen una criticidad y como estos en su actividad son adheridos a un plan de tratamiento de riesgos soportando los objetivos organizaciones.

- Frente a los riesgos presentes en los activos de la información de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón se determinó que inicialmente se identificaron riesgos con un alto porcentaje de criticidad que luego de la intervención por medio del tratamiento de riesgos disminuyo dicho porcentaje estableciendo los riesgos en un nivel aceptable avalado por la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

- De acuerdo a la necesidad de la curaduría se realizó la creación de políticas de seguridad aplicadas al interior de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón con base a la norma ISO/IEC 27001:2013 y avaladas por la dirección en reuniones establecidas con la alta Gerencia; lo que da cuenta de la importancia de realizar un trabajo en conjunto con las diversas áreas que hacen parte de los procesos misionales a fin de garantizar la seguridad de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón.

- Al implementar las políticas de seguridad al interior de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón, los funcionarios van a estar sujetos a cumplir diversos controles que garantizan la seguridad de la información de la curaduría.

- Con base en los controles y por medio de las políticas de seguridad de la información se estableció un mecanismo que apalanca los objetivos estratégicos del Core de negocio mitigando de este modo las vulnerabilidades que se presentan al interior de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón en relación con la seguridad de la información haciendo uso de las mejores prácticas soportadas por medio de la norma ISO/IEC 27001:2013.

- Respecto al plan de concienciación, se puede afirmar que la cultura organizacional en relación al cumplimiento de la políticas de seguridad implementadas con base en la Norma ISO/IEC 27001:2013, es una tarea que exige un compromiso por parte de la Dirección Administrativa, dado a que debe velar por hacer cumplir sin excepción estas directrices, se debe tener en cuenta que el incumplimiento de una política pactada puede comprometer los objetivos estratégicos del negocio y a su vez la continuidad del mismo, por lo anteriormente expuesto aunque la iniciativa inicial parte de la Dirección Administrativa es un trabajo en conjunto donde se involucra a todos los actores que conforman los procesos misionales en la Curaduría Urbana No. 3 Arq. Ana María Cadena Tobón.

- El plan de concienciación es un conjunto de actividades que deben ser ejecutadas con cierta periodicidad con el propósito de que se pueda mantener en el tiempo.

- Al momento de sustentar a la Dirección Administrativa los beneficios que traería diseñar y en un fututo implementar el Sistema de Gestión de Seguridad de la Información en la Curaduría Urbana No.3 Arq. Ana María Cadena Tobón, permitió tener una aceptación favorable porque es allí donde se comprendió que los riesgos se mitigan dado a que los activos de información se encuentran expuestos a diferentes amenazas, no óbstate esta aprobación parte de una aceptación de riesgo pactada por parte de la Dirección Administrativa.

- Retomando el punto de cultura organizacional es importante involucrar en todo tiempo al recurso humano que está involucrado directamente en los procesos

misionales en la Curaduría Urbana No. 3 Arq. Ana María Cadena Tobón toda vez que la socialización de cara a los usuarios se debe mantener en el tiempo, renovando las estrategias de socialización con el propósito de crear conciencia.

- El ejercicio de realizar el diseño de Gestión de Seguridad de la Información en la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón permitió integrar y trabajar de la mano con áreas como la Dirección Administrativa, la Coordinación del Sistema Integrado de Gestión (SIG) y Tecnología siendo esta un área transversal a los procesos en general de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón, entendiendo que al diseñar y posteriormente realizar la implementación del SGSI lo que se busca es proteger los activos de información de la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón agregando valor.

- El éxito rotundo del Sistema de Gestión de seguridad de la Información no recae sobre un área específica, es un trabajo de toda la Curaduría Urbana N.3 Arq. Ana María Cadena Tobón lograr que se mantenga en el tiempo con todos los criterios establecidos los cuales están sujetos a una mejora continúa haciendo uso de metodologías como el ciclo de (PHVA).

BIBLIOGRAFÍA

CAMPS, Rafael; CASILLAS, Luis; COSTAL, Dolors; GINESTÀ, Marc; ESCOFET, Carmen y MORA, Oscar. Software Libre. Bases de datos. Barcelona: Fundació per a la Universitat Oberta de Catalunya, 2005.p.63.

CISET. Centro de Innovación y Soluciones Empresariales y Tecnológicas. Firewall o cortafuegos. [en línea]. Bogotá: El Sitio [citado 8, enero, 2020]. Disponible en Internet: < URL: https://www.ciset.es/glosario/444-firewall>

COLEGIO NACIONAL DE CURADORES. ABC del Curador Urbano. [en línea]. Bogotá: El Sitio [citado 11, mayo, 2020]. Disponible en Internet: < URL: https://www.curadoresurbanos.org/abc-del-curador-urbano/>

COLOMBIA, CONGRESO DE LA REPUBLICA, Decreto 992 (4, junio, 1996). Por el cual se reglamenta el capítulo IV del decreto extraordinario 2150 de 1995. Bogotá: El Congreso, 1996.p.8.

CURADURÍA URBANA No. 3. Documento de Planeación Estratégica. Bogotá: La entidad. 2020.p.12.

_ _ _ _ _ _ _ _ . Informe Final de Gestión. Bogotá: La entidad. 2017.p.6.

_ _ _ _ _ _ _ _ La Curaduría. [en línea]. Bogotá: El Sitio [citado 23, agosto, 2020]. Disponible en Internet: < URL: http://curaduria3.com/quienes-somos/curaduria-urbana-no-3/>

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACION (ICONTEC). Gestión del riesgo. Principios y directrices. NTC-ISO 31000:2009. [en línea]. Bogotá, D.C.: El Instituto, 2011. p. 3.

_ _ _ _ _ _ _ _ Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. NTC-ISO-IEC 27001. Bogotá, D.C.: El Instituto, 2006. p. 3.

_ _ _ _ _ _ _ _ Tecnología de la Información. Técnicas de seguridad. Tecnología de la información técnicas de seguridad. Código de practica para la gestión de la seguridad de la información. Objeto. NTC-ISO-IEC 27002. Bogotá, D.C.: El Instituto, 2007. p. 1.

_ _ _ _ _ _ _ _ Tecnología de la Información. Técnicas de seguridad. Guía de implementación de un sistema de gestión de la seguridad de la información. Objeto. NTC-ISO-IEC 27003. Bogotá, D.C.: El Instituto, 2012. p. 1.

INTERNATIONAL STANDAR ORGANIZATION. ISO 27000. [en línea]. USA: La entidad [citado 3, junio, 2020]. Disponible en Internet: < URL: http://www.iso27000.es/glosario.html>

ISOTOOLS. ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información mediante el ciclo PHVA, Norma ISO 27001. [en línea]. España: El Sitio [citado 23, agosto, 2020]. Disponible en Internet: < URL: https://www.isotools.pe/iso-27001-implementacion-sistema-gestion-seguridad-informacion-ciclo-phva/>

KASPERSKY. Ingeniería social. [en línea]. Bogotá: El Sitio [citado 8, enero, 2020]. Disponible en Internet: < URL: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering>

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Glosario. [en línea]. Bogotá: El Ministerio [citado 8, enero, 2020]. Disponible en Internet: < URL: https://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7742.html>.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Computersecurity. 800-50. Gaithersburg. EE. UU, 2003.p.23.

ANEXOS

ANEXO A. ACTA DE REUNIÓN 1

ANA MARÍA CADENA TOBÓN
Curadora Urbana 3

ACTA DE REUNIÓN

LUGAR:	CURADURÍA URBANA 3

ASISTENTES

NOMBRE	CARGO
ALEJANDRA ALDANA LAMPREA	Cordinadora
ORLANDO ANGEL RODRIGUEZ	Director
JEISSON JAVIER GOMEZ TORRES	Administrador de Sistemas

TEMAS TRATADOS

Propuesta de intervencion para el diseño del SGSI para la Curadora Urbana 3.

Lanzamiento de propuesta de intervencion

Aprobacion de propuesta

COMPROMISOS ADQUIRIDOS

COMPROMISOS	FECHA ESTIMADA
La Direccion Administrativa autoriza el ingreso del Ing. John Castellanos quien realizara labores	Febreo 03-2020
para diseñar un Sistema de Gestion de Seguridad de la Informacion	

FECHA PROXIMA REUNION

OBSERVACIONES:

Las estradas a las instalaciones de la organización se realizaran de forma programada

ANEXO B. ACTA DE REUNION 2

ANA MARÍA CADENA TOBÓN
Curadora Urbana 3

ACTA DE REUNIÓN

LUGAR: CURADURÍA URBANA 3

FECHA: HORA:

ASISTENTES

NOMBRE	CARGO
MARIA FERNANDA MARTINEZ	Coordinadora de consultas y conceptos
DIANA LOZANO	Profesional gestión de la información
ADOLFO GOMEZ RIOS	Arquitecto de Análisis
JAIME DELGADO CAIPA	Arquitecto de Análisis
OSCAR MAHECHA	Notificador

ORDEN DEL DIA

Lanzamiento de propuesta de intervencion

TEMAS TRATADOS

Levantamiento de activos de información

Responsabilidades de los lideres

despliege fase 1

socializacion de cronograma

COMPROMISOS ADQUIRIDOS

COMPROMISOS	FECHA ESTIMADA
Levantamienot de inventario relacionado en archivo XLS	**Enero 31 2020**

FECHA PROXIMA REUNION

OBSERVACIONES:

Se entrega en fecha establecida

ANEXO C. ACTA DE REUNION 3

ANA MARÍA CADENA TOBÓN
Curadora Urbana 3

ACTA DE REUNIÓN

LUGAR: CURADURÍA URBANA 3

ASISTENTES

NOMBRE	CARGO
JEISSON JAVIER GÓMEZ TORRES	Administrador de sistemas
ALEJANDRO ROJAS GÓMEZ	Asesos de sistemas
JOHN CASTELLANOS	Consultor

ORDEN DEL DIA

Revision planes de trabajo

TEMAS TRATADOS

Levantamiento de requerimienots

Inventario de activos de informacion (dispositivos de comunicaciones)

Despliege fase 1

Socialización de cronograma

COMPROMISOS ADQUIRIDOS

COMPROMISOS	FECHA ESTIMADA
Levantamienot de inventario relacionado en archivo XLS	Enero 31 2020

FECHA PROXIMA REUNIÓN

OBSERVACIONES:

Se entrega en fecha establecida

ANEXO D. PROCEDIMIENTO DE RADICACION

ANA MARÍA CADENA TOBÓN
Curadora Urbana 3

PROCESO DE RADICACIÓN

OBJETO DEL PROCESO	ALCANCE DEL PROCESO
Realizar las actividades necesarias para la radicación de solicitudes de trámites de actuaciones urbanísticas.	Inicia desde el recibo de la solicitud del usuario y termina con el alistamiento del expediente y descarga para inicio de estudio.

POLÍTICAS DE OPERACIÓN Y ASPECTOS GENERALES

Oportunidad en la radicación y alistamiento de los expedientes
Aplicación de procedimientos internos
Aplicación del Protocolo de servicio al usuario
Propender por la optimización del tiempo en la radicación de los expedientes, con el fin de ofrecer un servicio oportuno al usuario, así como verificar la calidad de la información registrada en el sistema, siendo esta el insumo clave para el inicio y desarrollo de los demás procesos internos de la Curaduría.
Gestionar la radicación inmediata de los anexos a los expedientes para continuar con el respectivo trámite.

LÍDER DEL PROCESO

Profesional de Gestión de la información

Profesional de Gestión de la información

SECUENCIA E INTERACCIÓN

PROVEEDORES	ENTRADAS	PROCEDIMIENTOS	SALIDAS	USUARIOS
Usuarios	Documentos requeridos para la radicación según tipo de trámite	Radicación Inicial (CU3-PRC-RAD-01)	Registro expediente en el Sistema de Información	Proceso de Estudios Técnicos
			Expediente (documentos requeridos según tipo de trámite)	Proceso de Gestión de la Información y tecnología
Entidades Distritales Entes de Control	Normatividad, Requerimientos de información		Boleta de Facturación	Gestión contable
		Radicación Anexos (CU3-PRC-RAD-02)	Boleta de radicación, modelo valla	Usuarios
Proceso Gestión Admtiva y Gestión de la Dirección	Solicitudes de Información		Respuesta a requerimientos o solicitudes, Informes	Gestión de la Dirección
Proceso SIG y mejoramiento contínuo	Información SIG (Planeación, seguimiento, medición y mejora)		Informes de gestión Planes de mejoramiento	Proceso SIG y mejoramiento contínuo

RECURSOS

INFRAESTRUCTURA	TALENTO HUMANO	AMBIENTE DE TRABAJO
Equipos de Oficina, Equipos de Computo, Software, Instalaciones Físicas, Intranet. Internet, Teléfono y Fax.	Profesional Gestión de la Información Radicadores	Iluminación, ventilación, condiciones ergonómicas

RIESGOS	COMUNICACIÓN
* Radicación de expedientes en debida forma sin el cumplimiento del pleno de los requisitos * Ingreso de la información al sistema de información con errores que induzcan a un error de procedimiento *No generar alertas en casos que requieran especial atención	**Que:** Inquietudes presentadas en el proceso de radicación, informes **Quién:** Radicadores, Profesional de Gestión de la información **Cómo:** Verbalmente, correo electrónico **Cuándo:** Permanentemente **A quién:** Profesionales, Profesional de Gestión de la información, Profesional Atención usuarios, Director administrativo, Coordinador administrativo y SIG

CONTROLES EN EL PROCESO

* Ingreso de datos al sistema de información, verificando documentación física
* Verificación de la información al momento del alistamiento del expediente

INDICADORES DE GESTIÓN

NOMBRE DEL INDICADOR	FORMULA	TIPO
Tiempo en radicación	Días promedio del expediente en radicación	Eficiencia
Calidad en la radicación	# reprocesos por errores en radicación x 100 # exp. Radicados en el día	Eficacia

DOCUMENTOS APLICABLES

INTERNOS	EXTERNOS	REGISTROS
* CU3-PRC-RAD-01 Procedimiento de Radicación Inicial * CU3-PRC-RAD-02 Procedimiento de Radicación de Anexos * CU3-INS-GTI-01 Instructivo Alistamiento inicial exp y archivo de documentos *Protocolo de servicio al usuario (CU3-PRT-GSU-01)	Normatividad: * Decreto 1077 de 2015 * Resolución 1002 del 2010 * Decreto Distrital 514 de 2006 * Resolución 984 de 2005 * Ley General de Archivos 594 de 2000	* Boleta de radicación, formulario de solicitud, formulario de revisión del proyecto, modelo valla, boleta de facturación, planilla de radicaciones diarias y entrega, control de entrega de anexos, * Registro en el Sistema de Información * Documentación técnica y jurídica del expediente (Carpeta expediente) según tipo y modalidad del trámite

CODIGO	VERSIÓN No.	FECHA	DESCRIPCIÓN CAMBIO
CU3-PRO-RAD-01	0	14/12/2012	Versión preliminar del documento
CU3-PRO-RAD-01	1	11/03/2013	Versión inicial del documento
CU3-PRO-RAD-01	2	11/06/2015	Se incorpora el protocolo de atención al usuario, se amplían las políticas de operación, se ajustan indicadores.

ELABORÓ:	REVISÓ:	APROBÓ:
Alejandra Aldana Coordinadora administrativa y SIG	Orlando Rodríguez Director Administrativo	Ana María Cadena Tobón Curadora Urbana

ANEXO E. PROCEDIMIENTO DE RADICACIÓN INICIAL

ANA MARÍA CADENA TOBÓN
Curadora Urbana 3

PROCEDIMIENTO DE RADICACIÓN INICIAL

OBJETIVO	Recibir y verificar la documentación suministrada por el usuario para su radicación, de acuerdo al tipo de trámite a desarrollar.
DEFINICIONES	**Licencia urbanística:** Es el acto administrativo de carácter particular y concreto, expedido por el curador urbano o la autoridad municipal o distrital competente, por medio del cual se autoriza específicamente adelantar obras de urbanización y parcelación de predios, de construcción, ampliación, modificación, adecuación, reforzamiento estructural, restauración, reconstrucción, cerramiento y demolición de edificaciones, de intervención y ocupación del espacio público y realizar el loteo o subdivisión de predios. (Decreto 0019 de 2012 Art. 182) **Debida forma**: Se entenderá que una solicitud de licencia o su modificación está radicada en legal y debida forma si a la fecha de radicación se allega la totalidad de los documentos exigidos en el decreto 1077 de mayo 26 de 2015, aun cuando estén sujetos a posteriores correcciones. (Decreto 1077 de mayo 26 de 2015)

ORDEN	ENTRADA	FLUJOGRAMA	SALIDAS	RESPONSABLE	OBSERVACIONES Y/O PUNTOS DE CONTROL
1		Inicio Radicación			
2		Es Radicación inicial NO → Procedimiento Radicación Anexos SI			En el caso de que sea un traslado de expediente se solicita al usuario: Certificado de tradición y libertad, cambiar la primera hoja del formulario único de solicitud y si el titular es una fiducia debe aportar certificado de superintendencia financiera vigente. El auxiliar de archivo debe verificar que el usuario sea el titular o el apoderado (en este caso debe presentar el poder autenticado) , diligenciar el formato de solicitud de traslado- FT-103, para entrega al radicador, junto con los documentos correspondientes. El traslado debe llevar la aprobación de la profesional de gestión de la información y/o coordinadora Administrativa y del SIG. Se le debe informar al usuario el costo de la nueva radicación
3	Protocolo de servicio al usuario	Asignación turno de radicación	Sistema Información	Recepcionista	El horario de atención a los usuarios para radicación es de lunes a viernes de 8:00 a.m. a 5:00 p.m en jornada continua. En el caso de que sea traslado se asigna turno de radicación, archivo y notificación si se requiere.
4		Procedimiento Recepción y Atención usuarios		Recepcionista	
5	Protocolo de servicio al usuario Planilla asignación turnos	Atender al usuario según turno asignado		Radicador	Llamar al usuario por su nombre, saludar formalmente. Respetar turnos asignados
6	Formulario único de radicación Documentos jurídicos y técnicos	Identificar modalidad de la licencia requerida, verificar correcto diligenciamiento formulario	Formato de revisión e información de proyecto	Radicador	Para el caso de Prórroga, revalidación, subdivisión urbana, licencia de urbanismo, modificación de licencia vigente de construcción y urbanismo, Vo. Bo. de propiedad horizontal, entre otras, se verificarán documentos correspondientes con fechas actualizadas, no es necesario diligenciar el formato de revisión e información de proyecto. El formulario único de radicación debe ser diligenciado por el usuario, a tinta, completamente y firmado por los profesionales responsables y titulares. (Formato externo) El Formato de revisión e información de proyecto es diligenciado por el radicador (Formato externo), en el caso de que el usuario no presente todos los documentos requeridos se realizará la anotación sobre los documentos pendientes en el campo de observaciones.
7	Formulario único de radicación Formato de revisión e información de proyecto Documentos técnicos y jurídicos soporte Listado de requisitos para solicitud de licencias urbanísticas y otras actuaciones CU3-LIS-RAD-01	Verificar documentos contra lista de chequeo de acuerdo al tipo de trámite	Listado de requisitos para solicitud de licencias urbanísticas y otras actuaciones CU3-LIS-RAD-01	Radicador	Verificar cédula de ciudadanía Verificar Certificado de Cámara de Comercio o Supertintendencia financiera Verificar la documentación entregada por el usuario según tipo de trámite Verificar que el poder se encuentre autenticado por el titular del predio. Verificar la vigencia y número del certificado de tradición y libertad vs formulario El chip de los recibos de impuesto predial deben coincidir con el formulario Verificar dirección registrada en los estudios técnicos (Ver aclaración 3 y 4)

ANA MARÍA CADENA TOBÓN
Curadora Urbana 3

PROCEDIMIENTO DE RADICACIÓN INICIAL

8	Formulario único de radicación	Verificar si es Bien de Interés Cultural, colindante o sector de interés cultural	Consulta SINUPOT	Radicador	Realizar la consulta en la página www.sdp.gov.co / SINU POT. En el caso en que aplique, verificar la entrega del Anteproyecto aprobado por el Ministerio de Cultura o entidad competente. En caso de Bien Colidante se solicitará el anteproyecto en el Acta de observaciones
9	Formulario único de radicación	Verificar si es VIS,VIP o ESTATAL		Radicador	Verificar al momento de la radicación si el proyecto a radicar es un proyecto de Vivienda de Interés Social, Vivienda de Interés prioritario en las modalidades Unifamiliar o Bifamiliar y proyectos que pertenezcan al estado, si el proyecto tiene alguna de las anteriores caracteristicas solicitar boleta de reparto tanto VIS, VIP como ESTATALES la cual es entregada al usuario por la curaduria asignada en el respectivo año.
10	Formulario único de radicación Formato de revisión e información de proyecto	Crear el expediente. Registrar en el Sistema de Información para asignar número de radicación (Módulo de Radicación - nuevo)**	Sistema de Información	Radicador	Se debe verificar el ingreso correcto de la información general del proyecto y **del usuario en el módulo de radicación**, igualmente se debe verificar ortografía, verificar el ingreso de las direcciones de acuerdo al boletín catastral. Diligenciar completamente los siguientes submódulos: -Trámite y usos, -Localización, -Titulares
11		Realizar categorización del expediente	Sistema Información		
12		Asignar profesional para estudio		Radicador	La asignación de profesionales se realizará de acuerdo a los criterios predefeinidos por la Curaduría, o por solicitud del usuario. Se debe consultar a los coordinadores. Si es traslado se deben asignar los mismos profesionales que revisaron el proyecton anterior, al igual que los casos de modificaciones de licencias vigentes expedidas por la curaduría.
13	Formulario único de radicación Formato de revisión e información de proyecto	Ingresar la información de los documentos aportados al sistema	Sistema de Información	Radicador	Verificar que en el sistema en el módulo de radicación el registro de la totalidad de los documentos radicados (Generales, específicos y adicionales), dejar en el Sistema la información de los documentos pendientes.
14	Sistema Información	Diligenciar registro para pago	Boleta para pago FT-008	Radicador	Diligenciar en el módulo documentos Radicación-Nuevo la totalidad de los datos de la boleta para pago y entregarla al titular para que pase a facturación y pueda realizar el pago del cargo fijo
15	Boleta para pago FT-008	Procedimiento de facturación CU3-PRC-CON-01	Factura	Cajera	
16		Se radicó en debida forma? SI NO			Verificar el cumplimiento de la debida forma (cumplimiento aclaración 3 y 4)
17		Se informa requerimientos pendientes y términos para complementar información			Informar al usuario los términos de vencimiento para la radicación de los documentos pendientes (30 días hábiles).
18	Factura	Registrar en el sistema de infomación la radicación en calidad de debida forma o no, imprimir y entregar boleta de radicación	Sistema de Información Boleta de Radicación (Solicitud de licencia urbanística)	Radicador	El titular del trámite o el apoderado debe registrar su nombre y firma en el formato de revisión e información proyecto (Ver aclaración 5) Para la entrega de la boleta de radicación se debe solicitar al usuario la segunda copia de la factura cancelada que le fue entregada en caja. El usuario debe firmar la boleta de radicación.
19		Impresión y entrega modelo de valla de información a vecinos.	Formato valla	Radicador	Verificar si el proyecto requiere valla y seleccionar la opción en el sistema. Verificar que la información impresa esté correcta de acuerdo a la información registrada en el expediente, debe contener los datos de todos los propietarios. Informar al usuario los términos y requisitos para la radicación de la valla (5 días hábiles, a partir de la radicación en debida forma)
20		Procedimiento Llamadas seguimiento expedientes			

ANA MARÍA CADENA TOBÓN
Curadora Urbana 3

PROCEDIMIENTO DE RADICACIÓN INICIAL

21	Instructivo Alistamiento Expedientes	Organizar carpeta, foliar documentos, marcar bolsa del expediente	Expediente	Radicador	Organizar el expediente según parámetros de archivo. Sellar todos los documentos, planos, estudios de suelos y memorias de cálculo Archivar en la carpeta del expediente los documentos de acuerdo a los lineamientos definidos en el Instructivo de organización documentos radicación y foliar. Ver Instructivo de Alistamiento Expedientes (CU3-INS-GTI-01)
22		Entregar expediente para continuar con la estación correspondiente	Sistema de Información Planilla control de mov.expediente FT-125	Radicador	Descargar en el sistema de información según corresponda: * "Radicación incompleta" y entregar a archivo; * Zonificación en la etapa de 1ra revisión en caso de radicación en debida forma y pasar al profesional encargado * Primera revisión y pasar al profesional encargado en caso de las Propiedades Horizontales, prórrogas o revalidaciones *Prórrogas Si es prórroga o revalidación y está en debida forma pasa a primera revisión jurídica, sino cuenta con debida forma pasa al Archivo *Si es PH y está en debida forma pasa a primera revisión arquitectura, sino cuenta con debida forma pasa al Archivo.
23		Fin Radicación			

CUADRO DE CONDICIONES, ACLARACIONES U OBSERVACIONES

Aclaración 2.
El número del expediente está conformado así: los dos últimos dígitos del año, el número de la Curaduría Urbana y el número consecutivo del expediente ejemplo: (15-3-1935). En cada cambio de vigencia se inicia un nuevo consecutivo.

Aclaración 3.
Para la revisión de los documentos debe remitirse al Listado de requisitos para solicitud de licencias urbanísticas y otras actuaciones CU3-LIS-RAD-01.
Documentos generales: En el caso en que el solicitante no adjunte el Certificado de Tradición y Libertad, el Boletín Catastral y los Certificados de Cámara y Comercio, estos deben ser consultados e impresos (consulta internet - VUC). En caso de dificultad de acceso a la página imprimir reporte y gestionar consulta posterior si es posible imprimirlos adjuntar al expediente y dar debida forma
Todos los planos y estudios especializados deben ir debidamente rotulados y firmados por profesional idóneo de acuerdo con el Título VI-Ley 400 de 1997.

Aclaración 4.
Documentos jurídicos: (formulario debidamente diligenciado, certificado de tradición y libertad, documentos de identificación, poder, copia impuesto predial, información vecinos. Es importante verificar que los datos queden correctamente ingresados al sistema (Nombres, direcciones, datos de contacto).
Documentos técnicos: verificar la entrega de la totalidad de los documentos técnicos (arquitectura: planos rotulados, acotados, con niveles, por lo menos dos cortes, fachadas, cuadro de áreas, dimensiones de vías, uso, localización) (ingeniería: planos rotulados, acotados, memorias, estudio de suelos o apiques, para el caso de muros confinados verificar ortogonalidad del proyecto) . Verificar que los documentos estén firmados por el profesional responsable registrado en el formulario de solicitud.
Nota: en caso de presentarse alguna duda con la recepción del proyecto, se debe solicitar la aclaración por parte del profesional responsable.

Aclaración 5.
En caso de presentarse dificultades de acceso al sistema para la impresión de la boleta de radicación, se debe emplear el formato Solicitud de licencia urbanística FT-003 (Cuando es radicación por primera vez) o la Boleta de radicación de documentos anexos FT-023. Una vez se reestablezca el sistema de debe ingresar la respectiva información del expediente.

NORMATIVIDAD APLICABLE

Decreto 1077 de 2015

CONTROL DE REGISTROS

CÓDIGO	NOMBRE	RESPONSABLE DILIGENCIAMIENTO	LUGAR ARCHIVO	CLASIFICACIÓN	TIEMPO RETENCIÓN	DISPOSICIÓN
FT-025	Planilla de asignación de turnos para radicación	Recepcionista	Recepción	Cronológico	8 días	Eliminación
NA	Formulario Unico de Radicación	Usuario	Archivo expedientes	Cronológico	5 años	Digitalización-Transferencia SDP
NA	Formato de revisión e información de proyecto	Radicador	Archivo expedientes	Cronológico	5 años	Digitalización-Transferencia SDP
NA	Documentos técnicos (planos, estudios de suelos, memorias de cálculo)	Radicador	Archivo expedientes	Cronológico	5 años	Digitalización-Transferencia SDP
NA	Documentos jurídicos (certificado de tradición y libertad, impuestos, recibos servicios públicos) según tipo de trámite	Radicador	Archivo expedientes	Cronológico	5 años	Digitalización-Transferencia SDP
FT-008	Boleta para Facturación	Radicador	Archivo expedientes	Cronológico	5 años	Digitalización-Archivo Curadora
NA	Formato Valla	Radicador	Archivo expedientes	Cronológico	5 años	Digitalización-Archivo Curadora
NA	Factura	Cajera	Archivo expedientes	Cronológico	5 años	Digitalización-Archivo Curadora
FT-003	Solicitud de licencia urbanística	Radicador	Archivo expedientes	Cronológico	5 años	Digitalización-Eliminación
FT-125	Planilla control de mov.expediente	Radicador	Archivo expedientes	Cronológico	1 año	Eliminación
NA	Sistema de Información	Radicador	Archivo expedientes	Cronológico	Permanente	Back up

ANA MARÍA CADENA TOBÓN
Curadora Urbana 3

PROCEDIMIENTO DE RADICACIÓN INICIAL

CODIGO	VERSIÓN No.	FECHA	DESCRIPCIÓN CAMBIO
CU3-PRC-RAD-01	0	17/09/2012	Versión preliminar
CU3-PRC-RAD-01	1	11/03/2013	Versión inicial
CU3-PRC-RAD-01	2	08/11/2013	Verificación y actualización de registros y procedimientos
CU3-PRC-RAD-01	3	10/08/2015	Se elimina el procedimiento de conceptos en cuanto al direccionamiento, se ajusta columna de observaciones y/o puntos de control, se elimina el formato de reporte de radicaciones (FT-011), Se actualizan los formatos utilizados, se elimina la conexión con el procedimiento de conceptos, se separa del procedimiento de radicación de anexos, y del procedimiento de gestión y control, se incluye el Formato de revisión e información de proyecto y se aclara el diligenciamiento del Formato único de radicación, se incluye observación para el caso de otras actuaciones urbanísticas y traslado, se incluye el Protocolo de servicio al usuario, se ajustan responsables y cargos

ELABORÓ:	REVISÓ:	APROBÓ:
Alejandra Aldana Coordinadora administrativa y SIG	Orlando Rodríguez Director Administrativo	Ana María Cadena Tobón Curadora Urbana

ANEXO F. PROCEDIMIENTO DE RADICACIÓN ANEXOS

ANA MARÍA CADENA TOBÓN
Curadora Urbana 3

PROCEDIMIENTO DE RADICACIÓN DE ANEXOS

OBJETIVO	Recibir y verificar los documentos para cumplimiento de la debida forma, del Acta de Observaciones y/o de Soportes pagos.
DEFINICIONES	**Debida forma**: Se entenderá que una solicitud de licencia o su modificación está radicada en legal y debida forma si a la fecha de radicación se allega la totalidad de los documentos exigidos en el Decreto 1077 de 2015, aun cuando estén sujetos a posteriores correcciones.

ORDEN	ENTRADA	FLUJOGRAMA	SALIDAS	RESPONSABLE	PUNTOS DE CONTROL
1		Inicio Radicación			
2		Es Radicación 1 vez? (NO / SI)			
3	Protocolo de servicio al usuario	Procedimiento Radicación Inicial		Recepcionista	Se indaga con el usuario el tipo de trámite que va a realizar Se verifica si el expediente está dentro de los tiempos para la radicación de anexos. (Ver aclaración 2)
4	Protocolo de servicio al usuario	Asignación turno de radicación*	Sistema de Información	Recepcionista	
5		Es para cumplimiento, debida forma? (SI / NO → A)		Radicador	
6	Protocolo de servicio al usuario Sistema de Información	Atender al usuario según turno asignado		Radicador	Llamar al usuario por su nombre, saludar formalmente.
7	Anexos	Identificar el tipo de documentación entregada por el usuario		Radicador	
8	Sistema de Información	Verificar términos y documentos entregados según relación de pendientes	Sistema de Información	Radicador	Verificar en el Módulo Radicación Anexos, que no se encuentren vencidos los términos del expediente. (30 días hábiles a partir de la fecha de radicación). En caso contrario informar para inicio de proceso de desistimiento.Revisar notas del sistema
9		Registrar en el sistema de información y sellar		Radicador	Sellar los documentos (fecha y número de expediente)
10		Registrar la debida forma o no, imprimir y entregar boleta de radicación → C	Boleta de Radicación Anexos	Radicador	
11		Procedimiento Llamadas seguimiento expedientes		Profesional Gestión de servicio al usuario	
12		A → Es cumplimiento de AO? (NO → B / SI)			

ANA MARÍA CADENA TOBÓN
Curadora Urbana 3

PROCEDIMIENTO DE RADICACIÓN DE ANEXOS

13		Verificar términos y documentos entregados según relación de pendientes		Radicador	Verificar que no se encuentren vencidos los términos del expediente. (30 días hábiles a partir de la fecha de recibo del Acta de Observaciones y/o 15 días hábiles adicionales en caso de solicitud de prórroga). En caso contrario informar para iniciar proceso de desistimiento. En caso de que el usuario requiera prórroga debe presentar el formato correspondiente.
14		Registrar en el sistema de información y sellar	Sistema de Información	Radicador	Módulo radicación Acta de Observaciones
17		Imprimir y entregar boleta de radicación → C	Boleta de Radicación Anexos	Radicador	Imprimir boleta de radicación para entrega al usuario y para anexar al expediente.
18		B → Soportes pagos?			
19		Verificar términos y documentos entregados	Sistema de Información	Radicador	Revisar que la fecha de vencimiento de términos no sea mayor a 30 días hábiles a partir de la fecha de recibo del cargo variable. En caso contrario informar para iniciar proceso de desistimiento
20	Impuestos	Revisión impuestos		Radicador	Consultar el Certificado de libertad para verificar si es exigible el pago del impuesto de plusvalía e informarle al usuario. Ver aclaración 3. En caso de que se presenten dudas deben comunicarse con el profesional correspondiente.
21		Registrar en el sistema de información y sellar	Sistema de Información	Radicador	
22		C → Generar reporte de anexos recibidos del sistema	Reporte diario de anexos recibidos	Radicador	Verificar la relación de la totalidad de anexos recibidos (número de planos y/o documentos)
23		Entrega a archivo	Reporte diario de anexos recibidos	Radicador	En el caso del impuesto de Delineación Urbana, entregar para revisión prioritaria al auxiliar de archivo.
24	Reporte diario de anexos recibidos	Procedimiento de Archivo documentos y anexos CU3-PRC-GTI-02		Aux. Archivo	
25		Fin			

CUADRO DE CONDICIONES, ACLARACIONES U OBSERVACIONES

Aclaración 1. -El horario de atención a los usuarios es de lunes a viernes de 8:00 a.m. a 5:00 p.m en jornada continua.

Aclaración 2. El usuario cuenta con los siguientes plazos:
-30 hábiles días a partir de la fecha de radicación inicial del proyecto para radicación en debida forma
-5 días hábiles a partir de la fecha de radicación en debida forma para radicar la foto de la valla
-30 días hábiles para dar cumplimiento al acta de observaciones y realizar solicitud de prórroga por 15 días más
-30 días hábiles para presentar soportes de pago de expensas e impuestos
-Para prórrogas, revalidaciones PH y subdivisión, el plazo es de 30 días calendario.

ANA MARÍA CADENA TOBÓN
Curadora Urbana 3

PROCEDIMIENTO DE RADICACIÓN DE ANEXOS

Aclaración 3: La revisión de pagos se realiza según el tipo de trámite, cuando los pagos se encuentren completos el expediente se debe reembolsar en bolsa roja:
-**Revalidación:**impuesto delineación

-**VIS:**
Unifamiliar y Bifamiliar: impuesto delineación ($0), Carta viabilidad (comunicación expensas), demás impuestos que aplique
Multifamiliar: Comunicación expensas, Factura, impuesto de delineación y demás impuestos que aplique

-**Urbanismo:** Comunicación expensas, Factura, no requiere impuesto delineación
-**Urbanismo y construcción:** Impuesto delineación, Cargo Variable, Factura y demás impuestos que aplique

Construcción:
Obra nueva, demolición, reconocimiento de construcción: impuesto de delineación, Cargo Variable, Factura y demás impuestos que aplique.
Modificación: Cargo Variable, Factura, Impuesto de delineación y demás impuestos que aplique.
Ampliacion, adecuación, Licencia de construcción- modificación: Cargo Variable, Factura, Impuesto delineación y demás impuestos que aplique.
Reforzamiento estructural: Cargo Variable, Factura, Impuesto delineación y demás impuestos que aplique.

-**Modificación licencia vigente:** Cargo Variable, Factura. Si es adecuación o modificación de volumetría requiere impuesto de delineación, si es solo modificación no requiere impuesto de delineación.
Nota general: Se debe verificar con el área jurídica si el expediente requiere pago de plusvalía.

NORMATIVIDAD APLICABLE
Decreto 1077 de 2015

NORMATIVIDAD APLICABLE
Decreto 1077 de 2015

CONTROL DE REGISTROS						
CÓDIGO	NOMBRE	RESPONSABLE DILIGENCIAMIENTO	LUGAR ARCHIVO	CLASIFICACIÓN	TIEMPO RETENCIÓN	DISPOSICIÓN
NA	Planilla de asignación de turnos para radicación	Recepcionista	Archivo expedientes	Cronológico	8 días	Eliminación
NA	Boleta de radicación	Radicador	Archivo expedientes	Cronológico	5 años	Transferencia SDP
NA	Documentos Anexos	Radicador	Archivo expedientes	Cronológico	5 años	Transferencia SDP
NA	Reporte diario de anexos recibidos	Radicador	Sistema de información	Cronológico	6 meses	Eliminación
NA	Sistema de Información	Radicador	Archivo expedientes	Cronológico	Permanente	Back -up

CODIGO	VERSIÓN No.	FECHA	DESCRIPCIÓN CAMBIO
CU3-PR-RAD-02	0	24/05/2013	Versión preliminar del documento
CU3-PR-RAD-02	1	09/09/2013	Versión inicial del documento
CU3-PR-RAD-02	2	11/06/2015	Se incluye direccionamiento al Procedimiento Seguimiento gestión segunda revisión, se modifica la columna de observaciones y/o modificaciones, se eliminan los pasos correspondientes al procedimiento de de Archivo documentos y anexos, se elimina el formato control de entrega de anexos, se ajustan cargos y responsables, se actualiza la normatividad

ELABORÓ:	REVISÓ:	APROBÓ:
Alejandra Aldana Coordinadora Administrativa y SIG	Orlando Rodríguez Director Administrativo	Ana María Cadena Tobón Curadora Urbana

ANEXO G. DIAGNOSTICO ISO 27001

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
			PONDERACIÓN	0%	0%	50%	100%	
			PROMEDIO TOTAL					26%
A.5			POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN					0%
	A.5.1		Orientación de la dirección para la gestión de la seguridad de la información	0%	0%	0%	0%	0%
		A.5.1.1	Políticas para la seguridad de la información					
		Control	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.		0%			
		A.5.1.2	Revisión de las políticas para la seguridad de la información					
		Control	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.		0%			
A.6			ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN					10%
	A.6.1		Organización interna	0%	0%	20%	0%	20%
		A.6.1.1	Roles y responsabilidades para la seguridad de la información					
		Control	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.			30%		
		A.6.1.2	Separación de deberes					
		Control	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.			50%		
		A.6.1.3	Contacto con las autoridades					
		Control	Se deben mantener contactos apropiados con las autoridades pertinentes.		0%			
		A.6.1.4	Contacto con grupos de interés especial					
		Control	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.		0%			

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
		A.6.1.5	Seguridad de la información en la gestión de proyectos					
		Control	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.		0%			
	A.6.2		Dispositivos móviles y teletrabajo	0%	0%	0%	0%	0%
		A.6.2.1	Política para dispositivos móviles					
		Control	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.		0%			
		A.6.2.2	Teletrabajo					
		Control	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.		0%			
A.7			SEGURIDAD DE LOS RECURSOS HUMANOS					33%
	A.7.1		Antes de asumir el empleo	0%	0%	0%	100%	100%
		A.7.1.1	Selección					
		Control	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.				100%	
		A.7.1.2	Términos y condiciones del empleo					
		Control	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.				100%	
	A.7.2		Durante la ejecución del empleo	0%	0%	0%	0%	0%
		A.7.2.1	Responsabilidades de la dirección					
		Control	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.		0%			
		A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información					
		Control	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones		0%			

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
			regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.					
		A.7.2.3	Proceso disciplinario					
		Control	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.		0%			
	A.7.3		Terminación y cambio de empleo	0%	0%	0%	0%	0%
		A.7.2.1	Terminación o cambio de responsabilidades de empleo					
		Control	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.		0%			
A.8			GESTIÓN DE ACTIVOS					32%
	A.8.1		Responsabilidad por los activos	0%	0%	40%	100%	70%
		A.8.1.1	Inventario de activos					
		Control	Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.			80%		
		A.8.1.2	Propiedad de los activos					
		Control	Los activos mantenidos en el inventario deben tener un propietario.				100%	
		A.8.1.3	Uso aceptable de los activos					
		Control	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.		0%			
		A.8.1.4	Devolución de activos					
		Control	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.				100%	
	A.8.2		Clasificación de la información	0%	0%	0%	0%	0%
		A.8.2.1	Clasificación de la información					
		Control	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada		0%			
		A.8.2.2	Etiquetado de la información					
		Control	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el		0%			

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
			etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.					
		A.8.2.3	Manejo de activos					
		Control	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.		0%			
	A.8.3		Manejo de medios	0%	0%	25%	0%	25%
		A.8.3.1	Gestión de medios removibles					
		Control	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.			50%		
		A.8.3.2	Disposición de los medios					
		Control	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.		0%			
		A.8.3.3	Transferencia de medios físicos					
		Control	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.		0%			
A.9			CONTROL DE ACCESO					50%
	A.9.1		Requisitos del negocio para control de acceso	0%	0%	0%	80%	80%
		A.9.1.1	Política de control de acceso					
		Control	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.		0%			
		A.9.1.2	Acceso a redes y a servicios en red					
		Control	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.				80%	
	A.9.2		Gestión de acceso de usuarios	0%	0%	27%	0%	27%
		A.9.2.1	Registro y cancelación					
		Control	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.		0%			
		A.9.2.2	Suministro de acceso de usuarios					
		Control	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o		0%			

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
			revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.					
		A.9.2.3	Gestión de derechos de acceso privilegiado					
		Control	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.			80%		
		A.9.2.4	Gestión de información de autenticación secreta de usuarios					
		Control	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.		0%			
		A.9.2.5	Revisión de los derechos de acceso de usuarios					
		Control	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.			50%		
		A.9.2.6	Retiro o ajuste de los derechos de acceso					
		Control	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.			30%		
	A.9.3		Responsabilidades de los usuarios	0%	0%	15%	30%	23%
		A.9.3.1	Uso de información de autenticación secreta					
		Control	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.			30%		
	A.9.4		Control de acceso a sistemas y aplicaciones	0%	0%	50%	90%	70%
		A.9.4.1	Restricción de acceso a la información					
		Control	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.		0%			
		A.9.4.2	Procedimiento de ingreso seguro					
		Control	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.		0%			
		A.9.4.3	Sistema de gestión de contraseñas					
		Control	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.			100%		
		A.9.4.4	Uso de programas utilitarios privilegiados					

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
		Control	Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.				80%	
		A.9.4.5	Control de acceso a códigos fuente de programas					
		Control	Se debe restringir el acceso a los códigos fuente de los programas.				100%	
A.10			CRIPTOGRAFÍA					0%
	A.10.1		Controles criptográficos	0%	0%	0%	0%	0%
		A.10.1.1	Política sobre el uso de controles criptográficos					
		Control	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.		0%			
		A.10.1.2	Gestión de llaves					
		Control	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.		0%			
A.11			SEGURIDAD FÍSICA Y DEL ENTORNO					50%
	A.11.1		Áreas seguras	0%	0%	29%	0%	29%
		A.11.1.1	Perímetro de seguridad física					
		Control	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.			100%		
		A.11.1.2	Controles de acceso físicos					
		Control	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.			50%		
		A.11.1.3	Seguridad de oficinas, recintos e instalaciones					
		Control	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.			50%		
		A.11.1.4	Protección contra amenazas externas y ambientales					
		Control	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.		0%			
		A.11.1.5	Trabajo en áreas seguras					
		Control	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.			30%		
		A.11.1.6	Áreas de despacho y carga					

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
		Control	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.		0%			
	A.11.2		**Equipos**	0%	0%	42%	100%	71%
		A.11.2.1	**Ubicación y protección de los equipos**					
		Control	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.			100%		
		A.11.2.2	**Servicios de suministro**					
		Control	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.				100%	
		A.11.2.3	**Seguridad del cableado**					
		Control	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño		0%			
		A.11.2.4	**Mantenimiento de equipos**					
		Control	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.			100%		
		A.11.2.5	**Retiro de activos**					
		Control	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.			50%		
		A.11.2.6	**Seguridad de equipos y activos fuera de las instalaciones**					
		Control	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.		0%			
		A.11.2.7	**Disposición segura o reutilización de equipos**					
		Control	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobreescrito en forma segura antes de su disposición o reuso.		0%			
		A.11.2.8	**Equipos de usuario desatendido**					
		Control	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.		0%			

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
		A.11.2.9	Política de escritorio limpio y pantalla limpia					
		Control	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.		0%			
A.12			SEGURIDAD DE LAS OPERACIONES					29%
	A.12.1		Procedimientos operacionales y responsabilidades	0%	0%	30%	100%	65%
		A.12.1.1	Procedimientos de operación documentados					
		Control	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.				100%	
		A.12.1.2	Controles de acceso físicos					
		Control	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.			50%		
		A.12.1.3	Gestión de capacidad					
		Control	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.			30%		
		A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación					
		Control	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.			100%		
	A.12.2		Protección contra códigos maliciosos	0%	0%	10%	0%	10%
		A.12.2.1	Controles contra códigos maliciosos					
		Control	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.			20%		
	A.12.3		Copias de respaldo	0%	0%	50%	0%	50%
		A.12.3.1	Respaldo de la información					
		Control	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.			100%		

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
	A.12.4		Registro y seguimiento	0%	0%	50%	0%	50%
		A.12.4.1	Registro de eventos					
		Control	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.			100%		
		A.12.4.2	Protección de la información de registro					
		Control	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.			100%		
		A.12.4.3	Registros del administrador y del operador					
		Control	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.		0%			
		A.12.4.4	Sincronización de relojes					
		Control	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.			100%		
	A.12.5		Control de software operacional	0%	0%	0%	14%	14%
		A.12.5.1	Instalación de software en sistemas operativos					
		Control	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.				100%	
	A.12.6		Gestión de la vulnerabilidad técnica	0%	0%	25%	0%	13%
		A.12.6.1	Gestión de las vulnerabilidades técnicas					
		Control	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.		0%			
		A.12.6.2	Restricciones sobre la instalación de software					
		Control	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.			50%		
	A.12.7		Consideraciones sobre auditorías de sistemas de información	0%	0%	0%	0%	0%
		A.12.7.1	Controles de auditorías de sistemas de información					
		Control	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas		0%			

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
			operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.					
A.13			**SEGURIDAD DE LAS OPERACIONES**					**4%**
	A.13.1		**Gestión de la seguridad de las redes**	**0%**	**0%**	**15%**	**0%**	**8%**
		A.13.1.1	**Controles de redes**					
		Control	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.			30%		
		A.13.1.2	**Seguridad de los servicios de red**					
		Control	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.		0%			
		A.13.1.3	**Separación en las redes**					
		Control	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.		0%			
	A.13.2		**Transferencia de información**	**0%**	**0%**	**0%**	**0%**	**0%**
		A.13.2.1	**Políticas y procedimientos de transferencia de información**					
		Control	Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.		0%			
		A.13.2.2	**Acuerdos sobre transferencia de información**					
		Control	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.			100%		
		A.13.2.3	**Mensajería electrónica**					
		Control	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.		0%			
		A.13.2.4	**Acuerdos de confidencialidad o de no divulgación**					
		Control	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.			50%		

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
A.14			ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS					46%
	A.14.1		Requisitos de seguridad de los sistemas de información	0%	0%	25%	0%	25%
		A.14.1.1	Análisis y especificación de requisitos de seguridad de la información					
		Control	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.		0%			
		A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas					
		Control	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.		0%			
		A.14.1.3	Protección de transacciones de los servicios de las aplicaciones					
		Control	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.			50%		
	A.14.2		Seguridad en los procesos de desarrollo y de soporte	0%	0%	29%	100%	64%
		A.14.2.1	Política de desarrollo seguro					
		Control	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.		0%			
		A.14.2.2	Procedimientos de control de cambios en sistemas					
		Control	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.		0%			
		A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación					
		Control	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.		0%			
		A.14.2.4	Restricciones en los cambios a los paquetes de software					
		Control	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben			50%		

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
			limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.					
		A.14.2.5	Principios de construcción de los sistemas seguros					
		Control	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.			30%		
		A.14.2.6	Ambiente de desarrollo seguro					
		Control	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.		0%			
		A.14.2.7	Desarrollo contratado externamente					
		Control	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.			100%		
		A.14.2.8	Pruebas de seguridad de sistemas					
		Control	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.			50%		
		A.14.2.9	Prueba de aceptación de sistemas					
		Control	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.				100%	
	A.14.3		Datos de prueba	0%	0%	50%	0%	50%
		A.14.3.1	Prueba de aceptación de sistemas					
		Control	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.			100%		
A.15			RELACIONES CON LOS PROVEEDORES					44%
	A.15.1		Seguridad de la información en las relaciones con los proveedores	0%	0%	50%	100%	75%
		A.15.1.1	Política de seguridad de la información para las relaciones con proveedores					
		Control	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.				100%	
		A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores					

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
		Control	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.		0%			
		A.15.1.3	Cadena de suministro de tecnología de información y comunicación					
		Control	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.			100%		
	A.15.2		Gestión de la prestación de servicios de proveedores	0%	0%	25%	3%	14%
		A.15.2.1	Seguimiento y revisión de los servicios de los proveedores					
		Control	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.		0%			
		A.15.2.2	Gestión de cambios en los servicios de los proveedores					
		Control	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.			50%		
A.16			GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN					17%
	A.16.1		Gestión de incidentes y mejoras en la seguridad de la información	0%	0%	25%	8%	17%
		A.16.1.1	Responsabilidades y procedimientos					
		Control	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.		0%			
		A.16.1.2	Reporte de eventos de seguridad de la información					
		Control	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.		0%			
		A.16.1.3	Reporte de debilidades de seguridad de la información					
		Control	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.		0%			

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
		A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.					
		Control	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.		0%			
		A.16.1.5	Respuesta a incidentes de seguridad de la información					
		Control	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.		0%			
		A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información					
		Control	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.		0%			
		A.16.1.7	Recolección de evidencia					
		Control	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.			50%		
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO							26%
	A.17.1		Continuidad de seguridad de la información	0%	0%	0%	24%	24%
		A.17.1.1	Planificación de la continuidad de la seguridad de la información					
		Control	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.		0%			
		A.17.1.2	Implementación de la continuidad de la seguridad de la información					
		Control	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.		0%			
		A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información					
		Control	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.		0%			
	A.17.2		Redundancias	0%	0%	25%	30%	28%

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
		A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.					
		Control	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.			50%		
A.18			CUMPLIMIENTO					23%
	A.18.1		Cumplimiento de requisitos legales y contractuales	0%	0%	50%	40%	45%
		A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales					
		Control	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización			100%		
		A.18.1.2	Derechos de propiedad intelectual					
		Control	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.				100%	
		A.18.1.3	Protección de registros					
		Control	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.			100%		
		A.18.1.4	Privacidad y protección de información de datos personales					
		Control	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.				100%	
		A.18.1.5	Reglamentación de controles criptográficos					
		Control	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.		0%			
	A.18.2		Revisiones de seguridad de la información	0%	0%	0%	0%	0%
		A.18.2.1	Revisión independiente de la seguridad de la información					
		Control	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y		0%			

CAPITULO ISO.	SUBCAPITULO ISO	NUMERAL ISO	TITULO ISO	NO APLICA	NO CUMPLE	CUMPLE PARCIALMENTE	CUMPLE	AVANCE
			los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.					
		A.18.2.2	Cumplimiento con las políticas y normas de seguridad					
		Control	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.		0%			
		A.18.2.3	Revisión del cumplimiento técnico					
		Control	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.					