DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI – PARA LOS PROCESOS CRÍTICOS DE OFIMARCAS TOMANDO COMO GUÍA LA NORMA ISO 27001:2013.

DIEGO FERNANDO ROSAS LOPEZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA - ESCUELA DE INGENIERAS TIC
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2022

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI – PARA LOS PROCESOS CRÍTICOS DE OFIMARCAS TOMANDO COMO GUÍA LA NORMA ISO 27001:2013.

DIEGO FERNANDO ROSAS LOPEZ

Proyecto para optar al título de
Especialista en Seguridad Informática

Asesor
JENNY ALEJANDRA VARELA SEGURA
Docente

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA - ESCUELA DE INGENIERAS TIC
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2022

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del jurado

Firma del jurado

Bogotá ,30 – Octubre - 2022

Gracias a mi familia por el apoyo necesario para realizar las actividades y dar cumplimiento a la realización del proyecto.

AGRADECIMIENTOS

Mi mayor agradecimiento a la compañía Ofimarcas, por brindarme la oportunidad de realizar el proyecto dentro de su organización, por el apoyo y la asignación de recursos necesarios para cumplir con cada una de las metas que se definieron.

A mis compañeros de oficina por el apoyo ante las dudas y situaciones de incertidumbre que se presentaron.

CONTENIDO

	pág.
INTRODUCCIÓN	15
1. JUSTIFICACIóN	16
2. PLANTEAMIENTO DEL PROBLEMA	17
2.1 DESCRIPCIóN DEL PROBLEMA	17
2.2 FORMULACIóN DEL PROBLEMA	17
3. OBJETIVOS	18
3.2 OBJETIVO GENERAL	18
3.3 OBJETIVOS ESPECíFICOS	18
4. TIPO DE INVESTIGACIÓN	19
5. HIPÓTESIS	20
6. VARIABLES	21
6.1 VARIABLES INDEPENDIENTES	21
6.2 VARIABLES DEPENDIENTES	21
7. MARCO TEÓRICO	22
7.1 SGSI	22
7.1.1 Alcance de un SGSI	22
7.1.2 Beneficios de un SGSI	22
7.1.3 Política de un SGSI.	22
7.1.4 Evaluación de riesgos	22
7.1.5 Declaración de aplicabilidad	22
7.1.6 Tratamiento de riesgos	23
7.1.8 Auditorías internas y revisiones de la dirección	23
7.2 SEGURIDAD DE LA INFORMACIÓN	23
7.3 NTC ISO 27001:2013	24
7.4 CICLO DE MEJORA CONTINUA	26
7.4.1 Plan.	26
7.4.2 Hacer.	27
7.4.3 Verificar.	27
7.4.4 Actuar.	27
7.5 GESTIÓN DE RIESGOS ISO31000:2018	27
7.5.1 Evaluación de riesgos.	27
7.5.2 Tratamiento de los riesgos	28
7.5.3 Seguimientos y revisiones	28
7.5.4 Registros e informes	28

7.6 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN GUÍA min tic. 28
7.7 FASES DE IMPLEMENTACIÓN de las POLÍTICAS 28
7.7.1 Desarrollo. 28
7.7.1 Revisión de política 29
7.7.2 Aprobación. 29
7.7.3 Cumplimiento 29
7.7.4 Comunicación 29
7.7.5 Monitoreo. 29
7.7.6 Mantenimiento. 29
7.7.8 Políticas específicas recomendadas para la implementación de controles 29
7.8 PLAN DE CAPACITACIóN Y SENSIBILIZACIóN GUÍA min tic 30
7.8.1 Sensibilización. 30
7.9 DISEÑO DEL PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN 30
7.9.1 Modelo 1. Centralizado 31
7.9.2 Modelo 2. Parcialmente descentralizado 31
7.10 DISEÑO DEL PLAN DE SENSIBILIZACIÓN 31

8. MARCO DE REFERENCIA 32
8.1 OFIMARCAS 32
8.2 rESEÑA HISTÓRICA 32
8.3 MISIÓN 32
8.4 VISIÓN 32
8.5 VALORES HUMANOS 32
8.6 ORGANIGRAMA OFIMARCAS 33
8.7 MAPA DE PROCESOS 34
8.7.1 Procesos estratégicos. 34
8.7.2 Procesos críticos. 34
8.7.3 Procesos de apoyo 34
8.7.4 Perfiles, funciones y responsabilidades. 35
8.8 MARCO LEGAL 35

9. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN OFIMARCAS 37
9.1 ASPECTOS GENERALES 37
9.2 ALCANCE 37
9.3 PROCESO DE PREVENTA 37
9.4 PROCESO DE VENTA 38
9.5 PROCESO DE POSVENTA 38
9.6 PROCESO DE SOPORTE 39

10. DISEÑO METODOLÓGICO 40
10.1 CONTEXTO ACTUAL DE OFIMARCAS EN ASPECTOS GENERALES DE LA NORMA iso27001:2013 40
10.2 ALCANCE DEL DIAGNOSTICO 40
10.3 METODOLOGÍA 40

10.4 DIAGNOSTICO INICIAL DE LOS DOMINIOS Y CONTROLES DE LA NORMA ISO/IEC 27001:2013 EN OFIMARCAS 42
10.4.1 A5 Políticas de seguridad de la información. 43
10.4.2 A6 Organización de la seguridad de la información 44
10.4.3 A7 Seguridad de los recursos humanos. 44
10.4.4 A8 Gestión de activos 46
10.4.5 A9 Control de acceso. 47
10.4.6 A10 Criptografía 48
10.4.7 A11 Seguridad física y del entorno 49
10.4.8 A12 Seguridad de las operaciones 50
10.4.9 A13 Seguridad de las comunicaciones 52
10.4.10 A14 Adquisición, desarrollo y mantenimiento de sistemas 53
10.4.11. A15 Relaciones con los proveedores 55
10.4.12 A16 Gestión de incidentes de seguridad de la información 57
10.4.13 A17 Aspectos de seguridad de la información de la gestión de continuidad de negocio 57
10.4.14 A18 Cumplimiento 58
10.5 INFORME DIAGNÓSTICO ACTUAL DE LOS DOMINIOS 60

11. ACTIVOS DE OFIMARCAS 62
11.1 IDENTIFICACIÓN, CLASIFICACIÓN Y VALORIZACIÓN DE LOS ACTIVOS DE INFORMACIÓN 62
11.2 clasificación y VALORACIÓN de activos de INFORMACIÓN en ofimarcas 64
11.3 CRITICIDAD DE LOS ACTIVOS DE información 65
11.4 IDENTIFICACIÓN DE ACTIVOS CRÍTICOS 67
11.5 IDENTIFICACIÓN DE AMENAZAS PARA LA SEGURIDAD DE LA INFORMACIÓN 68

12. ANÁLISIS DE RIESGOS PARA LOS ACTIVOS CRÍTICOS DE OFIMARCAS 70
12.1 METODOLOGÍA 70
12.2 PROBABILIDAD 70
12.3 IMPACTO 71
12.4 VALORACIÓN DE RIESGOS 71
12.5 MAPAS DE CALOR 72

13. TRATAMIENTO DE LOS RIESGOS 76
13.1 VALORACIÓN DE CONTROLES 76
13.2 EFECTIVIDAD DE CONTROLES 77
13.2.1 Efectividad del control frente a la probabilidad. 78
13.2.2 Efectividad del control frente al impacto. 78

14. POLÍTICAS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN 98
14.1 ALCANCE 98
14.2 RESPONSABILIDADES 98
14.3 POLÍTICA GENERAL 99

14.3.1 Políticas organización de la seguridad de la información 99
14.3.2 Seguridad de los recursos humanos 100
14.3.3 Gestión de activos 100
14.3.4 Control de acceso 102
14.3.5 Triptografía. 103
14.3.6 Seguridad física y del entorno 104
14.3.7 Seguridad de las operaciones 104
14.3.8 Seguridad de las comunicaciones 106
14.3.9 Adquisición, desarrollo y mantenimiento de sistemas 107
14.3.10 Relaciones con los proveedores 107
14.3.11 Gestión de incidentes de seguridad de la información 108
14.3.12 Aspectos de seguridad de la información de la gestión de continuidad de negocio. 109
14.3.13 Cumplimiento 109

15. PLAN DE SENSIBILIZACIÓN 111
15.1 INTRODUCCIÓN 111
15.2 OBJETIVO 111
15.3 ALCANCE 111
15.4 ROLES Y RESPONSABILIDADES 111
15.4.1 Gerencia. 111
15.4.2 Líderes de los procesos 111
15.4.3 Proveedores y/o Terceros 112
15.4.4 Colaboradores. 112
15.4.5 Grupo de comunicaciones 112
15.5 Metas 112
15.6 Población destino 112
15.7 recursos 113
15.8 DIVULGACIÓN 113
15.8.1 funcionarios internos 113
15.8.2 Aliados y terceros: 113
15.9 DESCRIPCIÓN TEmas sugeridos de sensibilización y capacitación 113
15.9.1 Contexto del SGSI. 113
15.9.2 Políticas del SGSI. 113
15.9.3 Incidentes de seguridad de la información 114
15.9.4 Aplicaciones seguras. 114
15.9.5 Escritorio limpio. 114
15.9.6 Backups 114
15.9.7 Fuga de información. 114
15.9.8 Fraude online. 114
15.9.9 Clasificación de la información. 115
15.9.10 Seguridad en smartphone. 115
15.9.11 Correo electrónico seguro. 115
15.9.12 Contraseñas seguras 116
15.9.13 Bloqueo de sesión. 116

15.9.14 Navegación segura. 116
15.9.15 Malware. 116
15.9.16 Phishing 116
15.9.17 Protección de datos personales. 116
15.10 FRECUENCIA de actividades 117
15.11 CRONOGRAMA DE ACTIVIDADES 118
15.11.1 Evaluación y resultados. 120
15.12 materiales de ejemplo 120
16. CONCLUSIONES 125
17. RECOMENDACIONES 126

BIBLIOGRAFÍA 128

ANEXOS 131

LISTA DE FIGURAS

pág.

Figura 1. SGSI. 23
Figura 2. Secciones ISO 27001:2013. 25
Figura 3. Ciclo Planear, Hacer, Verificar y Actuar (PHVA). 26
Figura 4. Fases. 30
Figura 5. Organigrama Ofimarcas. 33
Figura 6. Procesos Ofimarcas. 34
Figura 7. Diagrama de flujo proceso de preventa. 37
Figura 8. Diagrama de flujo proceso de venta. 38
Figura 9. Diagrama de flujo proceso de posventa. 38
Figura 10. Diagrama de flujo proceso de soporte. 39
Figura 8. Resultado diagnóstico inicial. 42
Figura 9. Nivel de cumplimiento de ISO 27001:2013 en Ofimarcas. 61
Figura 10.Flujo gestión de riesgos Ofimarcas. 70
Figura 11. Ejemplo 1. 120
Figura 12. Ejemplo 2. 121
Figura 13. Ejemplo 3. 121
Figura 14. Ejemplo 4. 122
Figura 15. Ejemplo 5. 122
Figura 16. Ejemplo 6. 123
Figura 17. Ejemplo 7. 123
Figura 18. Ejemplo 8. 124

LISTA DE CUADROS

pág.

Cuadro 1. Marco legal 36
Cuadro 2. Convenciones diagnóstico general. 40
Cuadro 3. Preguntas diagnóstico general. 41
Cuadro 4. Resultado diagnóstico general 42
Cuadro 5 Convenciones diagnostico dominios y controles. 42
Cuadro 6 Políticas de seguridad de la información. 43
Cuadro 7. Organización de la seguridad de la información 44
Cuadro 8. Seguridad de los recursos humanos. 45
Cuadro 9 Gestión de activos 46
Cuadro 10. Control de acceso. 47
Cuadro 11. Criptografía 49
Cuadro 12. Seguridad física y del entorno. 49
Cuadro 13. Seguridad de las operaciones. 51
Cuadro 14. Seguridad de las comunicaciones 52
Cuadro 15. Adquisición, desarrollo y mantenimiento de sistemas 54
Cuadro 16. Relaciones con los proveedores 55
Cuadro 17. Gestión de incidentes de seguridad de la información. 57
Cuadro 18. Aspectos de seguridad de la información de la gestión de continuidad de negocio. 58
Cuadro 19. Cumplimiento 58
Cuadro 20. Resumen por dominios en Ofimarcas 60
Cuadro 21. Activos de información Ofimarcas. 62
Cuadro 22. Medición de impacto 64
Cuadro 23. Preguntas para valorar la criticidad de los activos. 65
Cuadro 24. Valoración del nivel de criticidad de los activos en Ofimarcas. 65
Cuadro 25. Sistema de selección de activos. 67
Cuadro 26. Activos seleccionados para la gestión de riesgos. 67
Cuadro 27. Lista de amenazas de seguridad de la información. 68
Cuadro 28. Valoración de probabilidad. 71
Cuadro 29. Valoración de impacto. 71
Cuadro 30. Valoración de los riesgos y criterios de aceptación. 72
Cuadro 31 Identificación y valoración de riesgo inherente. 72
Cuadro 32. Valoración de los riesgos y criterios de aceptación. 76
Cuadro 33. Lista de controles aplicables para las amenazas. 76
Cuadro 34 Efectividad controles. 78
Cuadro 35. Valoración de controles para falla fluido eléctrico 78
Cuadro 36. Valoración de controles para acceso no autorizado 79
Cuadro 37. Valoración de controles para daño físico. 80
Cuadro 38. Valoración de controles para daño lógico. 80
Cuadro 39. Valoración de controles para denegación de servicio. 81
Cuadro 40. Valoración de controles para eliminación de la Información. 81

Cuadro 41. Valoración de controles para errores de mantenimiento. 82
Cuadro 42. Valoración de controles para error en configuración. 82
Cuadro 43. Valoración de controles para fallo de servicios de comunicaciones. 83
Cuadro 44. Valoración de controles para fuga de información. 83
Cuadro 45. Valoración de controles para ingeniería social. 85
Cuadro 46. Valoración de controles para interceptación de información. 85
Cuadro 47. Valoración de controles para interrupción de servicios. 86
Cuadro 48. Valoración de controles para modificación erada de la información. 87
Cuadro 49. Valoración de controles para perdida de dispositivos 87
Cuadro 50. Valoración de controles para indisponibilidad de la aplicación. 88
Cuadro 51. Valoración de controles para abuso de privilegios. 88
Cuadro 52. Valoración de controles para manipulación errada de equipos. 89
Cuadro 53. Aplicación de controles a los riesgos 91
Cuadro 54. Frecuencia temas sugeridos 117
Cuadro 55. Cronograma 119

LISTA DE ANEXOS

pág.

Anexo A. Presupuesto 131
Anexo B. Cronograma 132

INTRODUCCIÓN

En la actualidad las empresas se encuentran expuestas ante amenazas de tipo internas y externas que de materializarse pueden afectar la reputación, imagen, ingresos de la compañía o pueden ocasionar multas de entes regulatorios, estos escenarios se pueden presentar por vulnerabilidades que son explotadas por personas mal intencionadas, que al implementar diferentes tipos de ataques pueden afectar los pilares de la seguridad de la información como la confidencialidad, integridad y disponibilidad.

Ofimarcas es una compañía que provee servicios de impresión, digitalización y administración de documentos, cuentan con una gran experiencia dentro del mercado y en la actualidad busca continuar posicionándose como una compañía líder con la mejor disposición comercial y técnica, enfocada a suministrar soluciones eficientes que den respuesta eficaz a la necesidad de mejorar los procesos y reducir los costos de impresión a sus clientes, esto la convierte en un objetivo atractivo para delincuentes informáticos que conociendo la actividad comercial de Ofimarcas se pueden ver tentados a vulnerar su seguridad para obtener la información de los clientes o afectar la operación de la empresa con la utilización de malware o cualquier otro tipo de ataque, en la actualidad los delincuentes informáticos están en constate desarrollo de sus habilidades, por lo que se es necesario establecer medidas que logren mitigar los riesgos hasta un nivel aceptado por la compañía y generar una conciencia de seguridad dentro de sus empleados.

Durante el desarrollo de este proyecto se busca diseñar un sistema de gestión de seguridad de la información SGSI, enfocado en los procesos críticos de Ofimarcas, con la intención de conocer el estado actual de la compañía en lo relacionado a seguridad de la información dentro del marco de la norma ISO 27001:2013 realizando un diagnóstico inicial de los numerales de la norma, identificar las amenazas, vulnerabilidades que dada un probabilidad pueden generar un impacto dentro de la empresa, para posteriormente hacer una recomendación de controles, diseñar las políticas de seguridad de la información y proponer un plan de capacitación y sensibilización.

1. JUSTIFICACIÓN

Según el reporte de la revista portafolio en junio del 2021, los ataques cibernéticos tuvieron un incremento del 30% con relación al mismo periodo analizado durante el año 2020, este dato se basa en las noticias relacionadas con ataques informáticos, las ciudades que tuvieron una mayor afectación fueron Bogotá con 8355 casos, Medellín 1664 casos y Cali con 1569[1].

Esta es una problemática que estará presente para cualquier organización sin importar su tamaño o campo de acción y que dada la sofisticación de los ataques informáticos todas las compañías deberían fortalecer sus estrategias, políticas y actividades relacionadas con la seguridad de la información. En la actualidad la empresa Ofimarcas no cuenta un sistema de gestión de seguridad de la información (SGSI), esto genera una mayor incertidumbre y sensación de exposición ante ataques cibernéticos, la empresa es consciente de esta falencia por lo cual considera que es un momento oportuno para realizar el proyecto dentro de su organización. Contar con un sistema de gestión de seguridad de la información, demuestra un compromiso organizacional buscando brindar una mayor tranquilidad a sus socios, colaboradores y clientes.

Con el fin de garantizar la operación y cumplimiento de los objetivos de la empresa, el SGSI que se desarrollara en Ofimarcas buscara conocer un diagnóstico inicial de su estado en el ámbito de seguridad de la información, identificar activos de información, detectar amenazas, vulnerabilidades y plantear controles que permitan reducir el nivel de riesgo al que en la actualidad están expuestos, siguiendo como guía la norma ISO 27001;2013.

[1] DIARIO PORTAFOLIO. Aumentan en 30% los ataques cibernéticos en Colombia. [en línea]. Bogotá: La Empresa [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.portafolio.co/tendencias/aumentan-en-30-los-ataques-ciberneticos-en-colombia-553803>

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DESCRIPCIÓN DEL PROBLEMA

En la actualidad las empresas independientemente de su actividad económica disponen de activos de información que son importantes para la ejecución de sus actividades, los constantes avances a nivel tecnológico no solo se ven reflejados en la infraestructura de las empresas, los ataques cibernéticos cada vez son más sofisticados y buscan comprometer los intereses de las compañías a cambio de reconocimiento o recompensas económicas.

Ofimarcas es una empresa que busca ofrecer soluciones de tecnología a sus clientes, almacenando y procesando una gran cantidad de información que se convierte en su activo más importante y como cualquier otra compañía está expuesta a diferentes riesgos informáticos que puedan afectar la prestación de servicios a sus clientes.

Actualmente se identifica una problemática en Ofimarcas debido a que no cuenta con documentación que le permita realizar una adecuada gestión de seguridad de la información y la inexistencia de inventario de activos, gestión de riesgos, políticas y estrategias de sensibilización hacia sus funcionarios.

2.2 FORMULACIÓN DEL PROBLEMA

¿De qué manera se puede mejorar los procesos relacionados con la gestión de la seguridad de la información en los procesos críticos de Ofimarcas?

3. OBJETIVOS

3.2 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información para los procesos críticos de la empresa Ofimarcas, tomando como guía la norma ISO 27001;2013, que permita realizar un diagnóstico de su estado actual con base a la norma, documentar los activos de información, gestión de riesgos, políticas y plan de sensibilización.

3.3 OBJETIVOS ESPECÍFICOS

- Identificar el contexto general de Ofimarcas con base a los aspectos generales de la norma ISO 27001:2013.

- Realizar un diagnóstico del estado actual de seguridad de la información de los procesos críticos de Ofimarcas con base a los dominios y controles de la norma ISO 27001:2013.

- Identificar, clasificar y priorizar los activos de información de los procesos Ofimarcas.

- Realizar una identificación y análisis de riesgos de seguridad de la información con base a la norma ISO 31000:2018.

- Definir controles del anexo A de la norma ISO 27001:2013 para el tratamiento del riesgo inherente y así obtener el riesgo residual.

- Diseñar una política de seguridad de la información con base al modelo de seguridad y privacidad Min Tic vive digital.

- Diseñar un plan de sensibilización tomando como guía el modelo de seguridad y privacidad Min Tic vive digital.

4. TIPO DE INVESTIGACIÓN

El desarrollo del proyecto se plantea desde un estudio descriptivo.

Se determina que es descriptivo, debido a que durante la ejecución de las actividades se describe el estado actual de seguridad de la información de los procesos de Ofimarcas, tomando como guía la norma ISO 27001:2013, la experiencia laboral y conocimientos obtenidos en la especialización en seguridad informática.

5. HIPÓTESIS

Hi: El diseño de un sistema de gestión de seguridad de la información para los procesos críticos de Ofimarcas le permitirá contar con un diagnóstico actual e identificar sus riesgos y como tratarlos.

Ho: El diseño de un sistema de gestión de seguridad de la información para los procesos críticos de Ofimarcas no le permitirá contar con un diagnóstico actual e identificar sus riesgos y como tratarlos.

6. VARIABLES

6.1 VARIABLES INDEPENDIENTES

- Procesos.

6.2 VARIABLES DEPENDIENTES

- Diseño
- SGSI
- Controles
- Políticas de seguridad.

7. MARCO TEÓRICO

7.1 SGSI

Un SGSI es un conjunto de políticas, procedimientos y directrices junto a los recursos y actividades que se administran en conjunto por una organización, buscando proteger sus activos esenciales. Desde el estándar ISO/IEC 27001 un SGSI es un enfoque sistemático que busca definir, implementar, operar, monitorear y mejorar la seguridad de la información, de tal forma que se apalanque los objetivos de la organización[22] tal como se aprecia en la figura 1.

Es una herramienta de gestión de la que se dispone en la organización para controlar el ámbito de la seguridad de la información.

7.1.1 Alcance de un SGSI. Su alcance depende de donde se identifiquen y ubiquen los activos de información con mayor nivel de importancia, puede establecerse sobre procesos, áreas o funciones específicas dentro de una organización.

7.1.2 Beneficios de un SGSI. Mayor confianza y satisfacción sobre los clientes y partes interesadas en la organización.

- Gestión clara y estructurada de seguridad de la información.

- Gestión de activos de información de manera organizada, facilitando la mejora continua y el ajuste según los objetivos estratégicos de la organización.

- Disminución de los riesgos que ocasionen la pérdida o corrupción de información.

7.1.3 Política de un SGSI. A través de la política se establece el compromiso de la alta dirección con los objetivos de seguridad de la información de la organización y la mejora continua del sgsi.

7.1.4 Evaluación de riesgos. Un SGSI se establece que dentro de la organización se debe determinar el proceso más apropiado para la gestión de riesgos, se debe documentar una metodología o procedimiento, que explique cómo se identifican, analizan y priorizan los riesgos relacionados con los activos de información más relevantes dentro del alcance. Debe contar con revisiones y actualizaciones que permitan mantener un enfoque preventivo para la definición de controles que mitiguen los riesgos de seguridad de la información.

7.1.5 Declaración de aplicabilidad. Su función principal es lograr evidenciar cuales de los controles del anexo A de la ISO/IEC 27001 se aplican dentro del alcance y

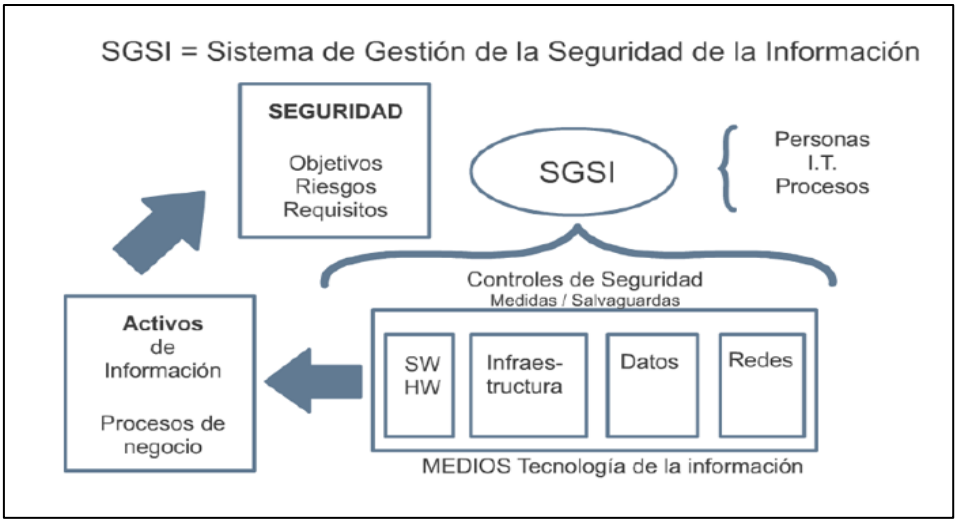
[2] ISO27001.es. Términos y Definiciones. [en línea]. Bogotá: La entidad [citado 3 de junio, 2022]. Disponible en Internet: < URL: https://www.iso27000.es/sgsi.html>

son los adecuados para la organización, así como los que no justifica su aplicación por su propio contexto, proceso o decisiones estratégicas.

7.1.6 Tratamiento de riesgos. Consiste en efectuar actividades de mitificación sobre aquellas situaciones no deseadas o inaceptables por la dirección. Cuando los riesgos son aceptables, es relevante contar con la firma del propietario del activo o del riesgo formalmente, de esta forma se acepta la responsabilidad de cualquier incidente que surja.

7.1.8 Auditorías internas y revisiones de la dirección. Los informes de auditoria son la evidencia más directa, de tal forma que se documentan los hallazgos, conclusiones y recomendaciones con el objetivo de comunicarse no conformidades y oportunidades de mejora.

Figura 1. SGSI.



Fuente: ENTERPRISE IT. SGSI. [en línea]. Bogotá: La entidad [citado 19 de noviembre, 2022]. Disponible en Internet: < URL: https://enterpriseit.cl/>

7.2 SEGURIDAD DE LA INFORMACIÓN

Seguridad de la información: Según la ISO 27000:2014[3], está definido como la preservación de la confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger la información y sistemas de información contra eventos que permitan el acceso, interrupción o destrucción de la información sin una autorización legitima[4].

[3] ISO/IEC 27000:2014. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información.
[4] NORMAS ISO 27001. Referencias normativas. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://normaiso27001.es/referencias-normativas-iso-27000/#terminos

La seguridad de la información busca salvaguardar la confidencialidad, integridad y disponibilidad de la información, estableciendo una serie de procedimientos, políticas y herramientas que permitan la gestión de acceso a la información en todas sus posibles formas de almacenamiento, implementando mecanismos de acceso físico y lógico, que permitan prevenir y detectar amenazas internas y externas que en caso de materializarse puedan afectar la operación y seguridad de las organizaciones. Se considera como un proceso de mejora continua, que requiere la participación de toda la organización, con actividades enfocadas en preservar los principios de la seguridad de la información, los cuales son:

- La disponibilidad: garantizar que la información pueda ser accedida en el momento que se requiera por personas autorizadas para ser consultada.

- La integridad: garantizar que la información solo sea modificada por el personal autorizado, mediante el uso de procesos que previamente fueron aprobados y así asegurar la precisión de los datos.

- La confidencialidad: es la acción de garantizar que la información solo pueda ser accedida por personal autorizado y así impedir que esta sea divulgada o publicada a personas ajenas o sin autorización.

- La trazabilidad: monitorear y rastrear cualquier actividad que se realiza sobre la información o sistemas de información.

- El no repudio: el fin de conocer exactamente los actores que participan en una transacción de tal forma que no puedan negarlo en ningún momento.

La seguridad de la información depende de la protección y seguridad de los activos de información, por esto es importante implementar controles, manteniendo un constante monitoreo y revisión de estos, buscando la mejora continua y le fortalecimiento de la seguridad de la información.

7.3 NTC ISO 27001:2013

La norma se elaboró con el fin de entregar una serie de lineamientos para establecer, implementar mantener y mejorar continuamente un sistema de gestión de seguridad de la información. Adoptar un SGSI dentro de una organización es una decisión estratégica, que busca apalancar los objetivos de la organización desde el ámbito de la seguridad de la información, generando una influencia en su establecimiento e implementación tomando como guía las necesidades, los requisitos de seguridad, el tamaño y estructura de la organización y todos los cambios que se puedan presentar a lo largo del tiempo en estos factores.

El SGSI busca preservar la confidencialidad, integridad y disponibilidad de la información, con la aplicación de la gestión de riesgos y brinda confianza a las partes

interesadas respecto a que los riesgos de seguridad son gestionados adecuadamente.

La norma específica los requisitos para establecer, implantar, documentar y evaluar un SGSI, a continuación, se muestra los puntos fundamentales:

- Definición del alcance del SGSI.
- Definición de una Política de Seguridad.
- Definición de una metodología y criterios para el Análisis y Gestión del Riesgo.
- Identificación de riesgos.
- Evaluación de los posibles tratamientos del riesgo.
- Desarrollo de un Plan de Tratamiento de Riesgos.
- Definición de métricas e indicadores de la eficiencia de los controles.
- Desarrollo de programas de concienciación en seguridad de la información.
- Gestión de recursos y operaciones.
- Gestión de incidencias.

Elaboración de procedimientos y documentación asociada[5]

A continuación, en la figura 2, se muestra las secciones que contempla la ISO 27001:2013.

Figura 2. Secciones ISO 27001:2013.

Fuente: Autor.

El sistema de gestión de seguridad de la información requiere de un proceso de mejora continua mediante el aprendizaje y la experiencia, por lo cual se platea el ciclo PHVA.

[5] ICONTEC. Instituto de Normas Técnicas y Certificación. Norma Técnica Colombiana. NTC-ISO-IEC 27001:2013. Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: Icontec. p.4

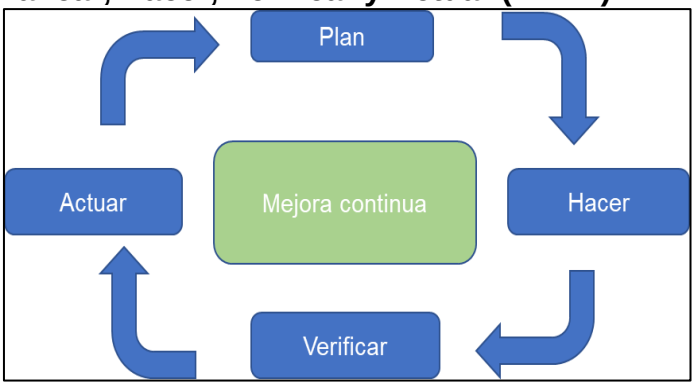
7.4 CICLO DE MEJORA CONTINUA

Planear, hacer, verificar y actuar. Para desarrollar un sistema de gestión de la seguridad de la Información SGSI con base en ISO 27001:2013, se recomienda utilizar un ciclo de mejora continua, definido dentro de la norma ISO 9001 del 2015. Esta metodología describe cuatro pasos esenciales, los cuales deben ejecutarse de forma sistemática logrando así la mejora en el proceso, buscando mejorar la calidad y aumentar la eficacia, la metodología, al ejecutarse de forma sistemática implica que, al ejecutarse la etapa final, se debe nuevamente iniciar con el ciclo, para cada vez incorporar nuevas mejoras[6].

La norma ISO 27001:2013, establece que debe existir una metodología de mejora continua, la cual permite que el sistema de seguridad de la información este en constante evolución, lo que facilita estar a la delantera de las amenazas a las que puede estar expuesta una empresa, adicional genera un mayor compromiso sobre las actividades a ejecutar por parte de los responsables de mantener el plan, permitiendo que se tenga una visual más amplia de su estado y el seguimiento de este.

El ciclo PHVA es una estrategia interactiva que permite la resolución de problemas buscando mejorar los procesos e implementar cambios. Es un método de mejora continua, este ciclo es una técnica útil para abordar, analizar y resolver problemas en las organizaciones, es una herramienta flexible de mejora iterativa (ver figura 3).

Figura 3. Ciclo Planear, Hacer, Verificar y Actuar (PHVA).



Fuente: Autor.

7.4.1 Plan. Esta primera fase permite determinar que debe hacerse y quien va a ser el responsable de ejecutar esas actividades, de ser necesarios se debe realizar el análisis del contexto de la organización dentro de la planificación, durante esta primera fase se debe definir.

[6] ISOTools. ¿En qué consiste el ciclo PHVA de mejora continua? [en línea]. Bogotá: La entidad [citado 19 de noviembre, 2022]. Disponible en Internet: < URL: https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/>

7.4.2 Hacer. Esta fase se refiere a la ejecución de las actividades que se planearon, la organización debe implantar la gestión de servicios para así gestionar de forma segura la información.

7.4.3 Verificar. Se debe supervisar y monitorear todos los objetivos definidos en el plan que se estableció en la organización e identificar si estos se cumplen de forma satisfactoria, los resultados de la verificación deben ofrecer información sobre el programa.

7.4.4 Actuar. Durante esta fase se debe mejorar la eficacia del programa, cualquier no conformidad identificada debe ser remediada con una definición clara de los responsables y actividades que se deben ejecutar para dar cumplimiento al ciclo de mejora continua. La compañía puede definir una serie de actividades que le permitan recolectar datos para llevar a cabo evaluaciones comparativas de las capacidades de la organización.

7.5 GESTIÓN DE RIESGOS ISO31000:2018

El propósito de la administración/gestión de riesgos es la creación y la protección del valor de los activos de información. Mejora el desempeño, fomenta la innovación y contribuye al logro de objetivos. Estos principios proporcionan una orientación sobre una gestión de riesgos efectiva y eficiente, comunicando su valor y explicando su intención y propósito[6].

7.5.1 Evaluación de riesgos. Consiste en el proceso global de identificación, análisis y evaluación de riegos:

- Identificación: Consiste en encontrar y describir los riesgos que podrían llegar a impedir que la organización logre el cumplimiento de los objetivos.

- Análisis: Es comprender la naturaleza de los riesgos y sus características, en caso de ser posible definir el nivel de estos. Es una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades y eventos.

- Evaluación: Implica comparar los resultados del análisis de riesgos con los criterios para determinar si se requiere realizar una acción adicional que puede ser:

- No hacer nada.
- Opciones de tratamiento de riesgos.
- Analizar nuevamente el riesgo para una mayor comprensión.
- Mantener los controles actuales.
- Reconsiderar objetivos[7].

[7] ISO. International Organization for Standardization. ISO 31000:2018. Gestión del riesgo — Directrices. [en línea]. Bogotá: La entidad [citado 12 de junio, 2022]. Disponible en Internet: < URL:

7.5.2 Tratamiento de los riesgos. Su propósito es seleccionar e implementar opciones para abordar los riesgos. Consiste en un proceso iterativo donde se debe:

- Formular y seleccionar las opciones para tratamiento de los riesgos.
- Plantear e implementar el tiramiento de los riesgos.
- Evaluar la efectividad del tratamiento.
- Analizar los riesgos residuales.
- Efectuar tratamientos adicionales.

7.5.3 Seguimientos y revisiones. Consiste en asegurar y mejorar la calidad del diseño, implementación y resultados del proceso de gestión de riesgos. Esta etapa debería ser una parte fundamental del proceso con responsabilidades definidas y apoyándose sobre el seguimiento y mejora continua.

7.5.4 Registros e informes. Los resultados deben ser documentados e informarse, estos registros buscan:

- Conocimiento en la organización del resultado de la gestión de riesgos.
- Información para toma de decisiones.
- Mejora continua.
- Apoyar la interacción de las partes interesadas con la gestión de riesgos.

Los reportes deberían lograr una mejor calidad de la interacción de las partes interesadas, apoyar la alta dirección y organismos de supervisión a cumplir sus necesidades.

7.6 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN GUÍA MIN TIC.

Es importante que las organizaciones definan las necesidades de los grupos de interés y la valoración de los controles que permitan mantener la seguridad de la información, se debe establecer una política que tenga como base el funcionamiento general de la organización, sus objetivos institucionales, sus procesos misionales y que esté aprobada por la dirección. La política debe ser concisa, fácil de leer y comprender, debe ser cumplida sin excepciones por todo el equipo de colaboradores[8].

7.7 FASES DE IMPLEMENTACIÓN DE LAS POLÍTICAS

7.7.1 Desarrollo. Durante esta fase se asigna el responsable de la creación de las

https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

[8] MinTIC. Ministerio de Tecnologías de la Información y Comunicaciones. Guía No. 2. Elaboración de la política general de seguridad y privacidad de la información. [en línea]. Bogotá: La entidad [citado 12 de junio, 2022]. Disponible en Internet: < URL: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>

políticas, estructurarlas, redactarlas, revisarlas y aprobarlas. Se debe realizar actividades enfocadas en los siguientes aspectos:

- Justificación: Por qué la entidad requiere contar con una política de seguridad de la información.

- Alcance: Definir la población, áreas, procesos y departamentos a los que aplica la política.

- Roles: Definir los responsables y roles para la implementación, aplicación, seguimiento y autorizaciones de la política.

7.7.1 Revisión de política. Una vez ha sido redactada, pasa por un proceso de evaluación de aplicabilidad, redacción y creación de las políticas de seguridad de la información.

7.7.2 Aprobación. Definir la persona o rol que tiene la competencia para formalizar la política.

7.7.3 Cumplimiento. Durante esta fase todas las políticas deben implementarse con relación a los controles de seguridad de la información, buscando una consistencia entre los controles implementados y los documentados.

7.7.4 Comunicación. En este punto se dan a conocer las políticas a todos los funcionarios y grupos de interés. Durante esta fase es importante obtener una retroalimentación de la efectividad de las políticas, de esta forma se logra realizar correcciones y ajustes que se consideren necesarios. Todos los funcionarios deben conocer la existencia de las políticas, su obligatoriedad de cumplimiento y la ubicación del documento.

7.7.5 Monitoreo. Las políticas deben ser monitoreadas para identificar su correcta aplicación, se pueden definir indicadores que permitan valorar su nivel de cumplimiento.

7.7.6 Mantenimiento. Consiste en mantener la política actualizada y que se ha ejecutado las correcciones que se han considerado.

7.7.8 Políticas específicas recomendadas para la implementación de controles

- Organización de la seguridad de la información.
- Gestión de activos.
- Control de acceso.
- No repudio.
- Privacidad y confidencialidad.
- Integridad.
- Disponibilidad del servicio e información.

- Registro y auditoría.
- Gestión de incidentes de seguridad de la información.
- Capacitación y sensibilización en seguridad de la información.

7.8 PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN GUÍA MIN TIC

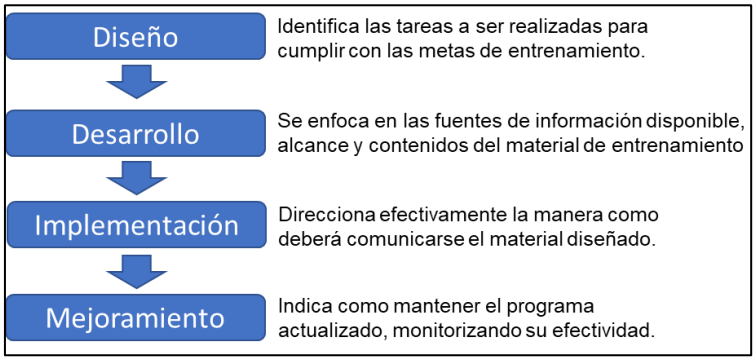
Según Mintic un programa de sensibilización y capacitación en seguridad de la información es efectivo cuando logra explicar manera apropiada las reglas adecuadas para el uso de los sistemas y la información. Generalmente estos procedimientos están plasmados en la política de seguridad de la información y requiere que se cumplan por parte de todos los funcionarios de una organización.

7.8.1 Sensibilización. Su principal objetivo es generar un impacto sobre el comportamiento de un grupo de personas, buscando reforzar buenas prácticas sobre un tema específico.

Ejemplo: Uso correcto de correo electrónico, consecuencias que se pueden presentar debido a la apertura y descarga de información adjunta en correos de orígenes no confiables.

Un plan de capacitación y sensibilización debe ejecutarse con base a las fases mostradas en la figura 4[9]:

Figura 4. Fases.



Fuente: MinTic.

7.9 DISEÑO DEL PLAN DE CAPACITACIÓN Y SENSIBILIZACIÓN

Su diseño debe realizarse teniendo en cuenta las necesidades y prioridades de la organización, se debe seleccionar el modelo de administración del plan.

[9] MinTIC. Ministerio de Tecnologías de la Información y Comunicaciones. Guía 14. Plan de Comunicación, Sensibilización, Capacitación. [en línea]. Bogotá: La entidad [citado 12 de junio, 2022]. Disponible en Internet: < URL: https://gobiernodigital.mintic.gov.co/portal/Categor-as/Seguridad-y-Privacidad-de-la-Informacion/150525:Plan-de-capacitacion-sensibilizacion-y-comunicacion-de-seguridad-de-la-informacion>

7.9.1 Modelo 1. Centralizado. Todas las actividades son responsabilidad por una entidad principal de la compañía, es decir la estrategia y la implementación son realizadas por un responsable principal y luego es distribuido de igual manera a todas las unidades organizaciones.

7.9.2 Modelo 2. Parcialmente descentralizado. Este modelo se caracteriza por la definición de las estrategias desde un ente principal y se delega la responsabilidad de implementación a cada una de las sedes por separado, de esta forma cada unidad organizacional asigna su presupuesto para el cumplimiento de las actividades definidas.

7.10 DISEÑO DEL PLAN DE SENSIBILIZACIÓN

Algunos de los elementos que deben encontrarse son:

- Políticas para que se ejecute un plan de capacitación y sensibilización.
- El alcance del programa.
- Metas por cumplir con el programa desarrollado.
- Audiencias objetivo para cada aspecto, quienes deben ser sensibilizados.
- Temas para tocar en cada sesión o cada curso.
- Frecuencia de las capacitaciones.
- Documentación y evidencia de cada aspecto del programa.
- Evaluación y renovación del material creado.

8. MARCO DE REFERENCIA

8.1 OFIMARCAS

Es una compañía fundada en 1989 que ofrece soluciones de impresión laser, copiado, digitalización y administración de documentos, su gran experiencia, le ha permitido posicionarse como un proveedor confiable y comprometido en satisfacer las expectativas y necesidades del mercado nacional, cuenta con un sólido soporte de posventa respaldado con un amplio stock de suministros y repuestos, tiene a disposición un departamento técnico con cobertura nacional, debidamente capacitado y certificado, para brindar satisfacción a las necesidades de las pequeñas y grandes empresas, en el sector corporativo, publicitario y el de artes gráficas[10].

8.2 RESEÑA HISTÓRICA

Desde 1994, es distribuidor de fábrica de la línea de impresoras y multifuncionales láser Kyocera, confiables escáneres de documentos Avision, Fujitsu y software especializado para la administración y el manejo de documentos.

8.3 MISIÓN

Proveer soluciones confiables y eficientes para la reproducción, transmisión, digitalización y administración de documentos, con productos y servicios de excelente calidad que permitan la disminución de los costos operativos y la satisfacción de las necesidades del mercado, en un proceso de desarrollo sostenido que reafirme día a día a Ofimarcas, como una empresa generadora de bienestar constante para sus clientes, empleados y asociados.

8.4 VISIÓN

Fortalecer permanentemente el liderazgo de Ofimarcas en el desarrollo y suministro de soluciones integrales para el procesamiento y administración de documentos, a través de una organización empresarial de excelente calidad humana y profesional, tomando como elementos fundamentales la continua capacitación del recurso humano y la actualización tecnológica del portafolio de productos, para mantener su sólido y competitivo posicionamiento en el mercado[10].

8.5 VALORES HUMANOS

En Ofimarcas saben que el mayor valor agregado es el equipo de colaboradores, promueven el permanente desarrollo de los valores humanos, teniendo como

[10] OFIMARCAS. Información Institucional. [en línea]. Bogotá: La entidad [citado 9 de octubre, 2022]. Disponible en Internet: < URL: https://www.ofimarcas.com/>

principios fundamentales:

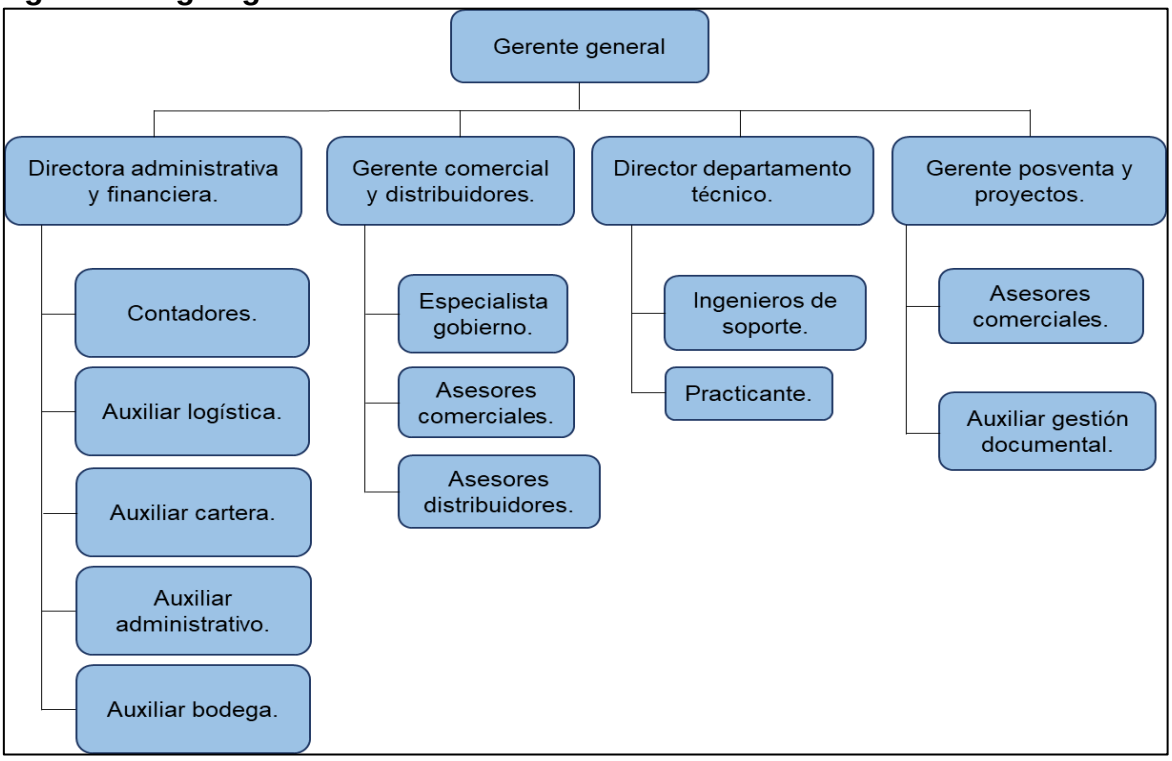
- Lealtad.
- Respeto.
- Compromiso.
- Ética profesional.

Están convencidos que la mejor forma de obtener un desarrollo económico y humano sostenido es hacer de la empresa una fuente generadora de bienestar constante.

8.6 ORGANIGRAMA OFIMARCAS

La estructura organizacional de Ofimarcas está encabezada por el gerente general quien lidera las actividades de los directores y gerentes de las diferentes áreas que conforman el gobierno de la compañía. Cada área tiene asignado sus respectivos, ingenieros, auxiliares, asesores comerciales y diferentes profesionales que ejecutan actividades enfocadas en el cumplimiento de objetivos de área, apalancando los objetivos generales de la compañía. En la figura 5 se muestra el organigrama de Ofimarcas.

Figura 5. Organigrama Ofimarcas.

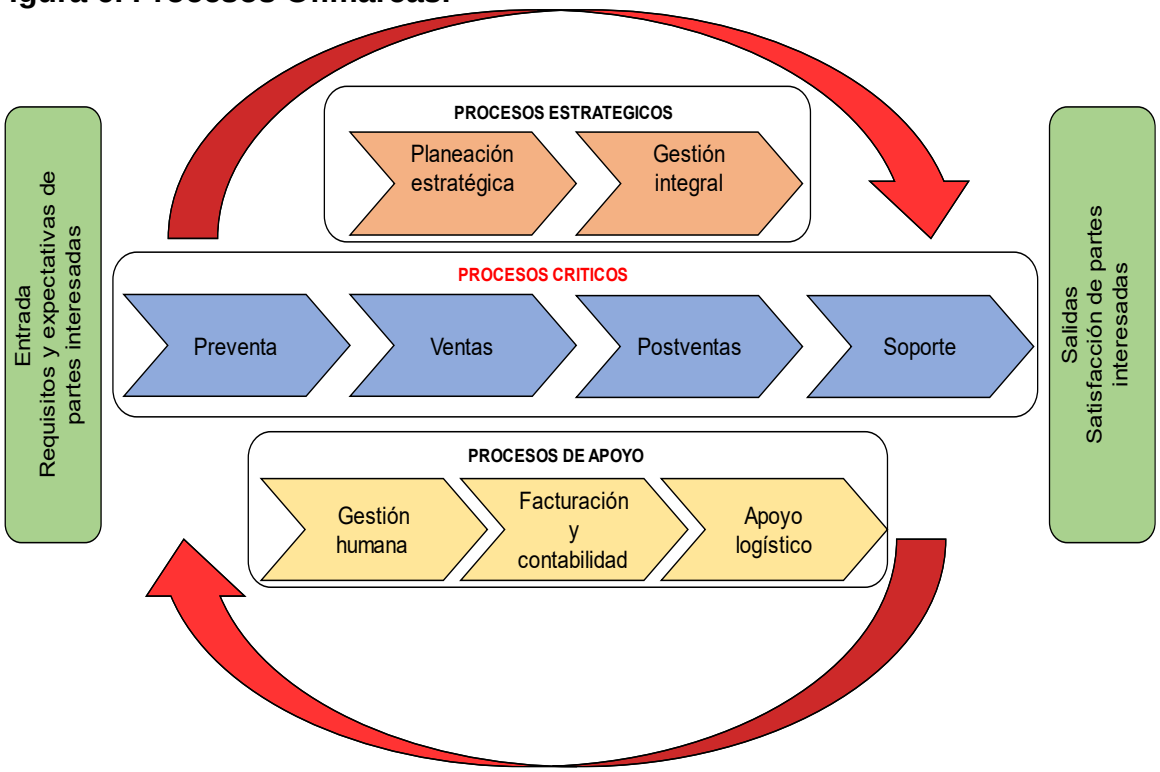


Fuente: OFIMARCAS. Información institucional interna. Bogotá, 2022.p.11.

8.7 MAPA DE PROCESOS

Para realizar las actividades dentro de la organización se requiere identificar de forma precisa los procesos que actualmente están definidos en Ofimarcas y los cuales intervienen de forma directa en los objetivos estratégicos de la compañía. En la figura 6, se relacionan y resalta los que son considerados como críticos:

Figura 6. Procesos Ofimarcas.



Fuente: OFIMARCAS. Información institucional interna. Bogotá, 2022.p.11.

8.7.1 Procesos estratégicos. Son los procesos desde donde la alta gerencia de Ofimarcas define los objetivos de negocio a cumplir, acompañado de las directrices y actividades a ejecutar para el cumplimiento de los objetivos.

8.7.2 Procesos críticos. Son los procesos operativos que aportan servicio al cliente durante la cotización, adquisición de equipos y posterior soporte de estos, para Ofimarcas estos son los procesos que contemplan los activos de información primordiales para la compañía y en los que se va a enfocar las actividades del proyecto.

8.7.3 Procesos de apoyo. Son los que se encargan de apoyar desde sus actividades los procesos operativos que entregan valor a los clientes y que los procesos critico o misionales cumplan con las expectativas de clientes e interesados de Ofimarcas.

8.7.4 Perfiles, funciones y responsabilidades.

- Gerente: Organizar, planear y dirigir todas las actividades de la empresa, con el objetivo de cumplir sus objetivos, económicos, organizaciones y de cumplimiento legal.

- Director administrativo: Planear, supervisar y controlar permanentemente la implementación de políticas administrativas y financieras que garanticen el óptimo funcionamiento de la compañía.

- Auxiliar administrativo: apoyar en todas las actividades que requiera la dirección administrativa.

- Contador: Recopilar, clasificar y registrar sistemáticamente, ordenada y oportunamente los hechos económicos de acuerdo con los principios contables y normas legales y tributarias las operaciones contables, con el propósito de tener una información financiera real, razonable y oportuna con el fin de facilitar los controles, análisis y toma de decisiones.

- Auxiliar de cartera: Desarrollar las funciones establecidas para recaudar la cartera propiedad de la empresa, optimizando el tiempo para responder a las solicitudes del cliente interno y externo, de manera que mejore el proceso y gestión del área.

- Auxiliar logística: Dar cumplimiento a las órdenes de compra de los clientes, garantizando los tiempos de entrega, realizar seguimiento y toma de inventario para garantizar el stock de equipos.

- Auxiliar bodega: Ejecutar labores relacionadas con la recepción, clasificación, almacenaje y despacho de mercancías.

- Ingeniero de soporte: Realizar actividades de mantenimiento a los equipos de clientes que así lo requieran.

8.8 MARCO LEGAL

Ofimarcas es una compaña legalmente constituida y da cumplimiento a los entes de control definidos por el gobierno de Colombia, se acoge a las normas que permiten la ejecución de su actividad económica, tal como se detalla en el cuadro 1.

Cuadro 1. Marco legal

Año	Ley	Entidad	Descripción de la norma
1979	Ley 9	Congreso de la República	Por medio de la cual se dictan medidas sanitarias[11]
1988	Ley 82	Congreso de la República	Por medio de la cual se aprueba el Convenio 159 sobre la readaptación profesional y el empleo de personas inválidas, adoptado por la Conferencia General de la Organización Internacional del Trabajo en su 69a. reunión, Ginebra, 1983.[12]
1988	Ley 46	Congreso de la Republica	Por la cual se crea y organiza el Sistema Nacional para la Prevención y Atención de Desastres, se otorga facultades extraordinarias al presidente de la República, y se dictan otras disposiciones.[13]
1990	ley 50	Congreso de la República	Por la cual se introducen reformas al Código Sustantivo del Trabajo[14]
1993	Ley 100	Congreso de la Republica.	Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones[15]
1997	Ley 378	Congreso de la Republica	Por medio de la cual se aprueba el "Convenio número 161, sobre los servicios de salud en el trabajo" adoptado por la 71 Reunión de la Conferencia General de la Organización Internacional del Trabajo, OIT, Ginebra, 1985.[16]
2001	Ley 717	Congreso de la Republica.	Por la cual se establecen términos para el reconocimiento de las pensiones de sobrevivientes y se dictan otras disposiciones.[17]
2002	Ley 776	Congreso de la Republica.	Por la cual se dictan normas sobre la organización, administración y prestaciones del Sistema General de Riesgos Profesionales.[18]
2002	Ley 769	Congreso de la República	Por la cual se expide el Código Nacional de Tránsito Terrestre y se dictan otras disposiciones[19]

Fuente: Elaboración propia a partir de los referentes citados al interior del cuadro

[11] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 9. (24, enero de 1979). Por medio de la cual se dictan medidas sanitarias. Bogotá, 1979. 39 p.

[12] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 82. (23, diciembre de 1982). Por medio de la cual se aprueba el Convenio 159 sobre la readaptación profesional y el empleo de personas inválidas, adoptado por la Conferencia General de la Organización Internacional del Trabajo en su 69a. reunión, Ginebra, 1983. Bogotá, 1982. 39 p.

[13] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 46. (2, diciembre de 1988). Por la cual se crea y organiza el Sistema Nacional para la Prevención y Atención de Desastres, se otorga facultades extraordinarias al presidente de la República, y se dictan otras disposiciones. Bogotá, 1988. 63 p.

[14] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 50. (28, diciembre de 1990). Por la cual se introducen reformas al Código Sustantivo del Trabajo y se dictan otras disposiciones. Bogotá, 1990. 51 p.

[15] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 100. (23, diciembre de 1993). Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones. Bogotá, 1990. 51 p.

[16] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 378. (9, julio de 1997). Por medio de la cual se aprueba el "Convenio número 161, sobre los servicios de salud en el trabajo" adoptado por la 71 Reunión de la Conferencia General de la Organización Internacional del Trabajo, OIT, Ginebra, 1985. Bogotá, 1997. 29 p.

[17] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 717. (24, diciembre de 2001). Por la cual se establecen términos para el reconocimiento de las pensiones de sobrevivientes y se dictan otras disposiciones. Bogotá, 2001. 29 p.

[18] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 776. (17, diciembre de 2002). Por la cual se dictan normas sobre la organización, administración y prestaciones del Sistema General de Riesgos Profesionales. Bogotá, 2002. 29 p.

[19] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 769. (6, julio de 2002). Por la cual se expide el Código Nacional de Tránsito Terrestre y e dictan otras disposiciones. Bogotá, 2002. 29 p.

9. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN OFIMARCAS

9.1 ASPECTOS GENERALES

Para Ofimarcas se establece un SGSI basado en el ciclo PHVA (planear, hacer, verificar y actuar), enfocado en los procesos denominados como críticos de la figura procesos Ofimarcas previamente mostrada, estos son los que apalancan los objetivos de la compañía. Los procesos de preventa, venta, posventa y soporte, al ser procesos claves se debe garantizar que los controles del análisis de riesgos, las políticas y plan de sensibilización se cumplan, se monitoreen y se realicen las modificaciones de tal forma que el SGSI tenga una maduración a lo largo del tiempo.

9.2 ALCANCE

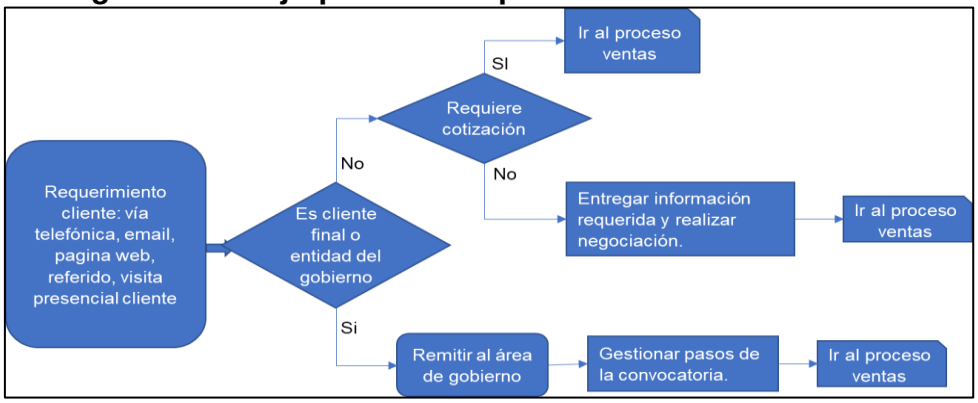
Según las características del negocio y sus activos de información se definió que las actividades del sistema de gestión de seguridad de la información se ejecutaran para los procesos críticos o misionales de preventa, venta, posventa y soporte, mostrados previamente en la figura procesos de Ofimarcas.

Para la compañía es de vital importancia el manejo que se da a los activos de información involucrados dentro de estos cuatro procesos. Durante la ejecución de las actividades de estos procesos existe interacción con los clientes por diferentes medios y es importante reducir los impactos operativos y de cumplimiento que pudieran verse afectados en el marco de la seguridad de la información.

9.3 PROCESO DE PREVENTA

Durante este proceso se ejecutan actividades que consisten en localizar clientes que pudieran necesitar de los equipos que ofrece Ofimarcas, tal como se aprecia en la figura 7.

Figura 7. Diagrama de flujo proceso de preventa.

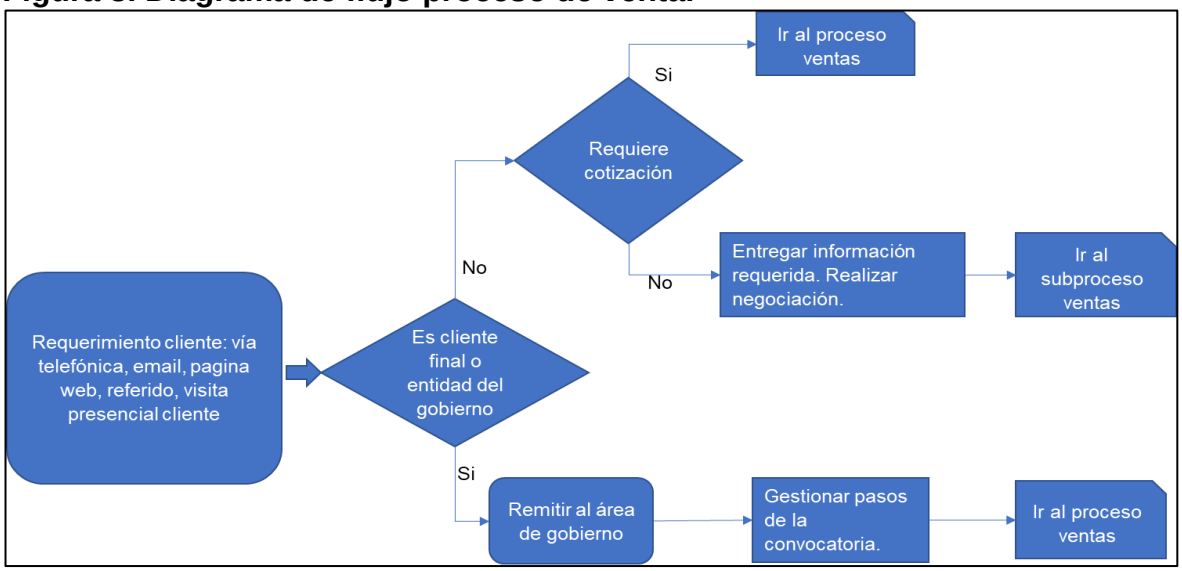


Fuente: OFIMARCAS. Información institucional interna. Bogotá, 2022.p.16.

9.4 PROCESO DE VENTA

Se realizan actividades y acercamientos con los clientes para lograr suplir sus necesidades y se concreta las ventas y diferentes aspectos como la logística de entrega, documentación legal y contratos de cumplimiento. (ver figura 8)

Figura 8. Diagrama de flujo proceso de venta.

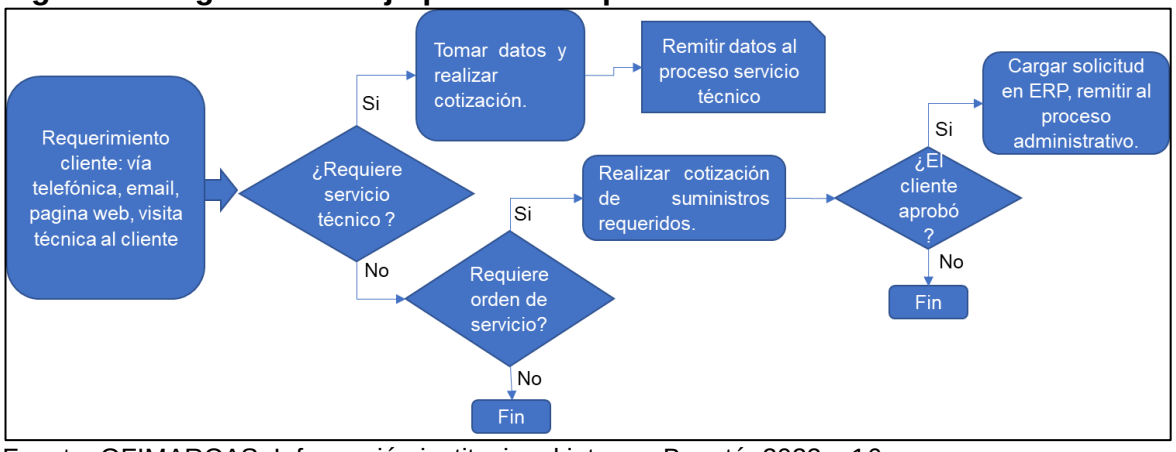


Fuente: OFIMARCAS. Información institucional interna. Bogotá, 2022.p.16.

9.5 PROCESO DE POSVENTA

Consiste en contactar a los clientes que ya adquirieron productos con Ofimarcas para verificar el correcto funcionamiento de los equipos y en caso de ser necesario se ofrecen soluciones dependiendo del tipo de escenario, nuevos productos o soporte. (ver figura 9)

Figura 9. Diagrama de flujo proceso de posventa.

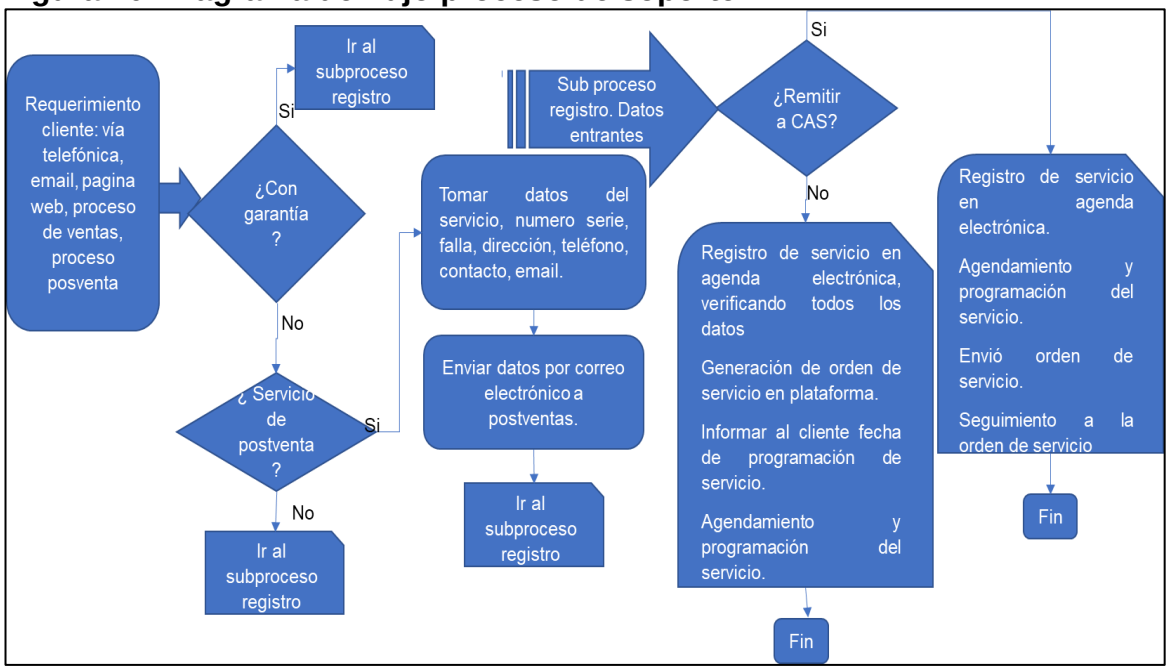


Fuente: OFIMARCAS. Información institucional interna. Bogotá, 2022.p.16.

9.6 PROCESO DE SOPORTE

Es el proceso mediante el cual se realizan actividades de mantenimiento y soporte para los equipos adquiridos por los clientes, este proceso se ejecuta ya sea por solicitud del cliente o por previa validación ejecutada por el proceso de posventa. (ver figura 10)

Figura 10. Diagrama de flujo proceso de soporte.



Fuente: OFIMARCAS. Información institucional interna. Bogotá, 2022. p.17.

10. DISEÑO METODOLÓGICO

10.1 CONTEXTO ACTUAL DE OFIMARCAS EN ASPECTOS GENERALES DE LA NORMA ISO27001:2013

Para conocer el contexto de cumplimiento de la norma ISO 27001:2013 dentro de Ofimarcas, se realizó una evaluación de los aspectos generales establecidos dentro de la norma, con el objetivo de identificar si existe la definición, ejecución y documentación de las actividades del sistema de gestión de seguridad de la información.

10.2 ALCANCE DEL DIAGNOSTICO

La evaluación interna se enfoca en los procesos críticos de Ofimarcas definidos en la figura procesos de Ofimarcas, mostrada previamente en el documento.

10.3 METODOLOGÍA

Se realizo una validación de la documentación actual de Ofimarcas con las áreas de tecnología, contabilidad, compras y facturación para identificar el nivel de cumplimiento de las generalidades de la norma ISO 27001:2013.

Se utilizo un cuadro de convenciones para identificar el estado actual dentro de Ofimarcas, que establece un estado según el nivel de cumplimiento y una sigla para dar respuesta a cada una de las preguntas del diagnóstico, tal como se aprecia en el cuadro 2.

Cuadro 2. Convenciones diagnóstico general.

Estado	Descripción	Sigla
Cumple satisfactoriamente	Se cumple 100% con lo establecido en la norma ISO 27001:2013, se encuentra documentado, se aplica y se monitorea.	CS
Cumple parcialmente	Se cumple de forma parcial lo establecido en la norma ISO 27001 versión 2013, se ejecuta de forma distinta, no se documentó, se aprobó, pero no se aplica.	CP
No cumple	No existe dentro de la empresa y/o actualmente no se hace.	NC

Fuente: ALCALDÍA MAYOR DE BOGOTÁ. informe de auditoría TIC Bogotá. [en línea]. Bogotá: La entidad [citado 9 de octubre, 2021]. Disponible en Internet: < URL: http://www.desarrolloeconomico.gov.co/transparencia/control/reportes-control-interno/informe-auditoria-proceso-gestion-tics-2021>

En el cuadro 3 se puede observar las preguntas que se respondieron con base a la validación de los aspectos generales de la norma ISO/IEC 27001:2013.

Cuadro 3. Preguntas diagnóstico general.

Pregunta	Valoración	Observación
¿Se definió un alcance del SGSI dentro de la organización?	CS	Para Ofimarcas es importante ejecutar las actividades del proyecto enfocado en los procesos misionales de la compañía, los cuales se definieron con la alta gerencia.
¿Ofimarcas tiene identificados los factores internos y externos que podrían afectar el proyecto?	CS	Desde la alta gerencia se cuenta con la aprobación de los recursos tecnológicos y humanos que permiten ejecutar las actividades del proyecto, para así minimizar eventos que pudieran afectar el proyecto.
¿Se identifico las expectativa y partes interesadas respecto al SGSI?	CS	Ofimarcas pertenece a un grupo empresarial el cual requiere que se inicie con un análisis de brechas en cuanto al estado actual de la compañía con base a las recomendaciones de la norma ISO27001:2013.
¿Se cuenta con la aprobación de la alta dirección de Ofimarcas para ejecutar las actividades del proyecto de SGSI?	CS	Al ser una recomendación del grupo empresarial al que pertenece Ofimarcas, se cuenta con aprobación por parte de la alta gerencia.
¿Existen políticas del SGSI aprobado por la alta dirección?	CP	La alta gerencia a definido políticas que se cumplen, sin embargo, estas deben estar documentadas y publicadas de tal forma que los colaboradores puedan acceder a ellas y entenderlas con facilidad.
¿Están definidos los roles, responsabilidades y autoridades de seguridad de la información?	CP	Desde los directores de cada área se identifican los roles y responsabilidades de cara al sistema de seguridad de la información sin embargo debe estar documentado y se le debe hacer seguimiento.
¿Está definido el proceso de identificación, valoración y tratamiento de riesgos de seguridad de la información?	CP	Se debe contar con una metodología que permita identificar, valorar y tratar los riesgos de seguridad de la información, aprobada por la alta dirección y documentada.
¿Existe un documento de aplicabilidad donde se definan los controles aplicables a la entidad?	NC	Se debe generar un documento de aplicabilidad donde se identifique y justifique a ellos controles que se incluyen y excluyen de la norma ISO27001:2013

Fuente: NORMA ISO/IEC 27001:2013.

En el cuadro 4, se muestra el resultado de las respuestas que fueron evaluadas conforme el nivel de cumplimiento actual de Ofimarcas, son 8 preguntas que representan el 100%, cada estado dependiendo del nivel de cumplimiento, se representó con su respectivo porcentaje de participación. Se logro identificar que el nivel de cumplimiento respecto a los aspectos generales de la norma es bajo, dado que algunas actividades se realizan, pero no se encuentran documentadas en Ofimarcas.

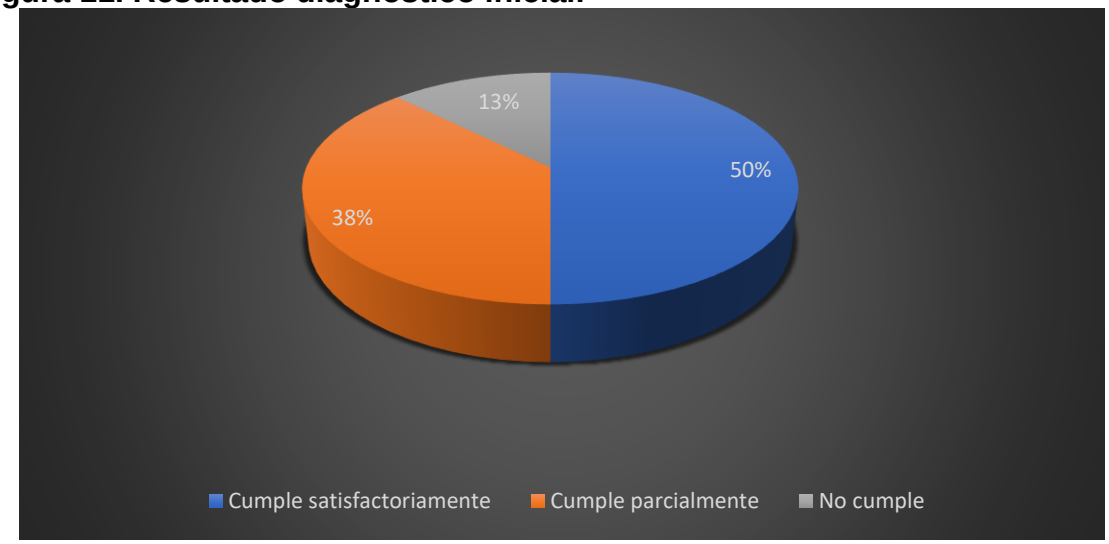
Cuadro 4. Resultado diagnóstico general

Ítem	Sigla	Cantidad	% Participación
Cumple satisfactoriamente	CS	4	50%
Cumple parcialmente	CP	3	38%
No cumple	NC	1	13%
Total		8	100%

Fuente: Autor.

En la figura 11 se representan los datos del cuadro anterior.

Figura 11. Resultado diagnóstico inicial.



Fuente: Autor.

10.4 DIAGNOSTICO INICIAL DE LOS DOMINIOS Y CONTROLES DE LA NORMA ISO/IEC 27001:2013 EN OFIMARCAS

Posterior a las preguntas generales con base a la norma ISO 27001:2013, se realizó la evaluación de cada uno de los dominios y controles que especifica la norma en conjunto con los lideres y directores de los procesos críticos para identificar si en la actualidad los controles se encuentran implementados, documentados y es aplicado en los procesos. La norma cuenta con 11 dominios cada uno de ellos con sus respectivos controles, el cuadro 5 de convenciones que se muestra a continuación permitió realizar la valoración según el nivel de cumplimiento que se definió en la descripción, de esta forma se evaluaron los controles.

Cuadro 5 Convenciones diagnostico dominios y controles.

Estado	Descripción	Sigla
Cumple satisfactoriamente	Existe, es gestionado, se está cumpliendo con lo que la norma ISO/IEC 27001 versión 2013 solicita, está documentado, es conocido y aplicado por todos los involucrados en el SGSI cumple 100%	CS

Cuadro 5 (Continuación)

Estado	Descripción	Sigla
Cumple parcialmente	Se cumple de forma parcial lo establecido en la norma ISO/IEC 27001 versión 2013, se ejecuta de forma distinta, no se documentó, se aprobó, pero no se aplica.	CP
No cumple	No existe dentro de la empresa y/o actualmente no se hace.	NC
No aplica	No se aplica en la Entidad	NA

Fuente: ALCALDÍA MAYOR DE BOGOTÁ. informe de auditoría TIC Bogotá. [en línea]. Bogotá: La entidad [citado 9 de octubre, 2021]. Disponible en Internet: < URL: http://www.desarrolloeconomico.gov.co/transparencia/control/reportes-control-interno/informe-auditoria-proceso-gestion-tics-2021>

Dentro de Ofimarcas existen controles que no aplican dada la naturaleza del negocio, es importante tener presente que no cuentan con área de desarrollo de software y adicional dentro de la compañía no existen actividades con medios removibles, por este motivo no aplican los controles A.8.3.3, A.9.4.5, A.12.1.4, A.14.2.1, A.14.2.2, A.14.2.6, dentro del diagnóstico de los controles se va a estipular su estado como No aplica.

10.4.1 A5 Políticas de seguridad de la información. Este dominio busca que desde la alta dirección de Ofimarcas se defina y apruebe una política de seguridad de la información, que sea comunicada a los colaboradores y partes externas, generando así un documento que este aliado a los requisitos del negocio, las leyes y reglamentos pertinentes. Estas políticas deben ser revisadas y valorar las oportunidades de mejora en respuesta a los cambios del entorno organizacional, las circunstancias del negocio, las condiciones legales o el ambiente técnico. (ver cuadro 6)

Cuadro 6 Políticas de seguridad de la información.

A.5 Políticas de la seguridad de la información			Estado
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información			
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.			
A.5.1.1	Políticas de 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 partes externas pertinentes.	CP
A.5.1.2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continuas.	NC

Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.2 A6 Organización de la seguridad de la información. El objetivo de este dominio es contar con un marco de referencia que permita iniciar y controlar la implementación y operación de la seguridad de la información dentro de Ofimarcas. (ver cuadro 7)

Cuadro 7. Organización de la seguridad de la información

A.6 Organización de la seguridad de la información			Estado
A.6.1 Organización interna			
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.			
A.6.1.1	Seguridad de la información Roles y responsabilidades	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	CP
A.6.1.2	Separación de deberes	Control: Las tareas 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.	CP
A.6.1.3	Contacto con las autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes.	CP
A.6.1.4	Contacto con grupos de interés especial	Control: Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	CS
A.6.1.5	Seguridad de la información en gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	CP
A.6.2 Dispositivos móviles y teletrabajo			Estado
Objetivo: Garantizar* la seguridad del teletrabajo y el uso de dispositivos móviles.			
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.	CP
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.	CP

Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.3 A7 Seguridad de los recursos humanos. El dominio está dirigido a garantizar que los colaboradores y contratistas comprenden con claridad sus responsabilidades y que cuentan con las habilidades para dar cumplimiento a los roles que se les asignen, Ofimarcas debe contar con procedimientos que permitan realizar valoraciones, antes de la contratación, durante la permanencia del colaborador en la organización y cuando finaliza su relación contractual con la

compañía. El dominio requiere un trabajo colaborativo entre el área de gestión humana y el área jurídica, es importante contar con un plan de formación y sensibilización que genere una cultura de seguridad entre las partes interesadas. (ver cuadro 8)

Cuadro 8. Seguridad de los recursos humanos.

A.7 Seguridad de los recursos humanos			Estado
A.7.1 Antes de asumir el empleo			
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.			
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, reglamentos 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.	CP
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 seguridad de la información.	CP
A.7.2 Durante la ejecución del empleo			**Estado**
Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			
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 de la organización.	CP
A.7.2 Durante la ejecución del empleo			**Estado**
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 regulares sobre las políticas y procedimientos pertinentes para su cargo.	CP
A.7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal y comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	CP
A.7.3 Terminación y cambio de empleo			**Estado**
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.			
A.7.3.1	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.	NC

Fuente: Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.4 A8 Gestión de activos. El principal objetivo es identificar los activos de información de Ofimarcas y definir las responsabilidades de protección adecuadas. Deben existir reglamentos que permitan un uso aceptable de los activos, procedimientos para la devolución de activos, los activos deben ser calificados según su función en cuanto a requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada, adicional se debería desarrollar e implementar procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación que considere Ofimarcas. (ver cuadro 9)

Cuadro 9 Gestión de activos

A.8 Gestión de activos			**Estado**
A.8.1 Responsabilidad por los activos			
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.			
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.	CP
A.8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben ser propios.	CP
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.	CP
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.	CP
A.8.2 Clasificación de la información			**Estado**
Objetivo: Asegurar que la organización recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.			
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.	NC
A.8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	NC
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.	NC
A.8.3 Manejo de medios de soporte			**Estado**
Objetivo: Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.			
A.8.3.1	Gestión de medios de soporte removibles	Control: Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	CP

Cuadro 9 (continuación)

A.8.3 Manejo de medios de soporte			Estado
A.8.3.2	Disposición de los medios de soporte	Control: Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	CP
A.8.3.3	Transferencia de medios de soporte físicos	Control: Control Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	NA

Fuente: Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.5 A9 Control de acceso. Limitar el acceso a información y a instalaciones de procesamiento de información de Ofimarcas, la organización debe contar con un procedimiento y una política de control de acceso basado en los requisitos de la compañía y de la seguridad de la información, dentro de los procedimientos se debe controlar el acceso a redes y servicios en red, gestión de acceso de los usuarios, registro, ajuste y cancelación de usuarios. Los usuarios deben tener claridad en cuanto a que son los responsables de rendir cuentas por salvaguardar sus credenciales de acceso. (ver cuadro 10)

Cuadro 10. Control de acceso.

A.9 Control de acceso			Estado
A.9.1 Requisitos del negocio para control de acceso			
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			
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.	CP
A.9 Control de acceso			**Estado**
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.	CP
A.9.2 Gestión de acceso de usuarios			**Estado**
Objetivo: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.			
A.9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación del registro, para posibilitar la asignación de los derechos de acceso.	CP
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 cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	CP
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.	CP

Cuadro 10 (continuación)

A.9.2 Gestión de acceso de usuarios			Estado
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.	CP
A.9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los dueños de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	NC
A.9.2.6	Cancelación 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 cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	CP
A.9.3 Responsabilidades de los usuarios			**Estado**
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.			
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.	CP
A.9.4 Control de acceso a sistemas y aplicaciones			**Estado**
Objetivo: Prevenir el uso no autorizado de sistemas y de aplicaciones.			
A.9.4.1	Restricción de acceso a 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.	CP
A.9.4.2	Procedimiento de conexión segura	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.	CP
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	NC
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	CP
A.9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a códigos fuente de programas.	NA

Fuente: Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.6 A10 Criptografía. El dominio busca que se dé un uso apropiado y eficaz de la criptografía para proteger la confidencialidad y la integridad de la información. Ofimarcas debe contar con una política que defina controles criptográficos que permitan proteger la información que se considere necesaria, se debe realizar una valoración para identificar si una solución criptográfica es apropiada y que tipo de control se debería aplicar, para que propósito y a que procesos. (ver cuadro 11)

Cuadro 11. Criptografía

A.10 Criptografía			Estado
A.10.1 Controles criptográficos			
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de información.			
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 protección de información.	NC
A.10.1.2	Gestión de claves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.	NC

Fuente: Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.7 A11 Seguridad física y del entorno. El dominio busca que las compañías definan y utilicen perímetros de seguridad que permitan proteger áreas donde se procese o almacene información sensible, Ofimarcas debe contar con controles de acceso físico en oficinas, recintos e instalaciones, implementar medidas contra amenazas externas y ambientales, para sus áreas de despacho y carga, contar con equipos que permitan proteger la red eléctrica ante fallas de energía y otras interrupciones de los servicios de suministro. Adicionalmente se debe contar con procedimientos que permitan ubicar y proteger los equipos para reducir los riesgos de amenazas, documentar y realizar movimientos únicamente bajo las aprobaciones que se consideren necesarias. (ver cuadro 12)

Cuadro 12. Seguridad física y del entorno.

A.11 Seguridad física y ambiental			Estado
A.11.1 Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			
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.	CP
A.11 Seguridad física y ambiental			**Estado**
A.11.1.2	Controles físicos de entrada	Control: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	CP
A.11.1.3	Seguridad de oficinas, salones e instalaciones	Control: Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	CP
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.	CS
A.11.1.5	Trabajo en áreas seguras	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	CS

Cuadro 12 (continuación)

A.11.1.6	Áreas de despacho y carga	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.	CP
A.11.2 Equipos			**Estado**
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.			
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 ambientales, y las posibilidades de acceso no autorizado.	CP
A.11.2.2	Servicios públicos de soporte	Control: Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.	CP
A.11.2 Equipos			**Estado**
A.11.2.3	Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.	CS
A.11.2.4	Mantenimiento de equipos	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	CP
A.11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	CP
A.11.2.6	Seguridad de equipos y activos fuera del predio	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.	CP
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 con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	CP
A.11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	CP
A.11.2.9	Política de escritorio y pantalla limpios	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	CP

Fuente: Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.8 A12 Seguridad de las operaciones. Asegurar la ejecución de la operación de manera correcta y segura, Ofimarcas debe contar con procedimientos documentados y estar a disposición de todos los usuarios que los requieran, debe existir un control de cambios para los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que pudieran afectar la seguridad

de la información, se debe realizar seguimiento constante a los recursos necesarios para asegurar el desempeño y hacer las proyecciones sobre la capacidad necesaria para un correcto funcionamiento de los sistemas. (Ver cuadro 13)

Cuadro 13. Seguridad de las operaciones.

A.12 Seguridad de las operaciones			Estado
A.12.1 Procedimientos operacionales y responsabilidades			
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.			
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.	CP
A.12.1.2	Gestión de cambios	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.	CP
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.	CP
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operacionales	Control: Se deben separar los ambientes de desarrollo, prueba y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.	NA
A.12.2 Protección contra códigos maliciosos			**Estado**
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.			
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.	CP
A.12.3 Copias de respaldo			**Estado**
Objetivo: Proteger contra la pérdida de datos.			
A.12.3.1	Copias de 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.	CP
A.12.4 Registro y seguimiento			**Estado**
Objetivo: Registrar eventos y generar evidencia.			
A.12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	NC
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.	NC
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.	NC

Cuadro 13 (continuación)

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.	NC
A.12.5 Control de software operacional			**Estado**
Objetivo: Asegurarse de la integridad de los sistemas operacionales.			
A.12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	NC
A.12.6 Gestión de la vulnerabilidad técnica			**Estado**
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.			
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.	NC
A.12.6.2	Restricciones sobre la instalación de software	Control: Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.	CP
A.12.7 Consideraciones sobre auditorías de sistemas de información			**Estado**
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.			
A.12.7.1	Controles sobre auditorías de sistemas de información	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	NC

Fuente: Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.9 A13 Seguridad de las comunicaciones. El dominio busca que se asegure la información en la red y durante su procesamiento, Ofimarcas debe gestionar sus redes y controlarlas para proteger la información, los sistemas y aplicaciones, debe existir segmentación de redes. Adicionalmente deben existir procedimientos para proteger la información dentro de la organización y al momento de ser transmitidas con entidades externas, se debe utilizar mecanismo y acuerdos de confidencialidad. (ver cuadro 14)

Cuadro 14. Seguridad de las comunicaciones

A.13 Seguridad de las comunicaciones			**Estado**
A.13.1 Gestión de la seguridad de redes			
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			
A.13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	CS

Cuadro 14 (Continuación)

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.	CS
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.	CP
A.13.2 Transferencia de información			**Estado**
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.			
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.	CP
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.	CP
A.13.2 Transferencia de información			**Estado**
A.13.2.3	Mensajes electrónicos	Control: Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	CP
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.	CP

Fuente: Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.10 A14 Adquisición, desarrollo y mantenimiento de sistemas. Ofimarcas Se debe asegurar que la seguridad de la información sea una parte integral durante el todo el ciclo de vida de los sistemas. El aseguramiento se debe realizar para nuevos sistemas o para mejoras en los actuales, se debe asegurar la información que se transmite a través de redes públicas ante actividades fraudulentas, divulgación o modificación no autorizada, la organización debe implementar control de cambios para todos los sistemas que se utilicen, así como restricciones en los cambios de los paquetes de software. (ver cuadro 15)

Cuadro 15. Adquisición, desarrollo y mantenimiento de sistemas

A.14 Adquisición, desarrollo y mantenimiento de sistemas			Estado
A.14.1 Requisitos de seguridad de los sistemas de información			
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	CP
A.14 Adquisición, desarrollo y mantenimiento de sistemas			**Estado**
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	CS
A.14.1.3	Protección de transacciones de servicios de aplicaciones	Control: La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir 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.	CS
A.14.2 Seguridad en los procesos de desarrollo y de soporte			**Estado**
Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			
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.	NA
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.	NA
A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales.	CP
A.14.2 Seguridad en los procesos de desarrollo y de soporte			**Estado**
A.14.2.4	Restricciones sobre cambios en los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	CP
A.14.2.5	Principios de organización de sistemas seguros	Control: Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.	NC
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	NA

Cuadro 15 (continuación)

A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratada.	NC
A.14.2.8	Pruebas de seguridad de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba y criterios relacionados.	NC
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 y criterios relacionados.	CS
A.14.3 Datos de prueba			**Estado**
Objetivo: Asegurar la protección de los datos usados para pruebas.			
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	CS

Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.11. A15 Relaciones con los proveedores. El objetivo del dominio es asegurar los activos de información a los cuales tiene acceso los proveedores. Ofimarcas debe realizar acuerdos con los proveedores de tal forma que se garantice a seguridad de la información y así mitigar los riesgos asociados con el acceso de los proveedores. (ver cuadro 16)

Cuadro 16. Relaciones con los proveedores

A.15 Relaciones con los proveedores			**Estado**
A.15.1 Seguridad de la información en las relaciones con los proveedores			
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.			
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.	CS
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	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.	CP
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.	CP
A.15.2 Gestión de la prestación de servicios de proveedores			**Estado**
Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.			

Cuadro 16 (Continuación)

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.	CP
A.15.2.2	Gestión de cambios a 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.	CP
A.16 Gestión de incidentes de seguridad de la información			**Estado**
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información			
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.			
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.	CP
A.16.1.2	Informe 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.	CP
A.16 Gestión de incidentes de seguridad de la información			**Estado**
A.16.1.3	Informe 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 e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	NC
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.	CP
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.	CP
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.	CP
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.	CP

Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.12 A16 Gestión de incidentes de seguridad de la información. El dominio busca que las organizaciones logren un enfoque coherente y eficaz para gestionar los incidentes de seguridad de la información que se puedan presentar, incluyendo la comunicación de los eventos de seguridad, Ofimarcas debe contar con responsabilidades y procedimientos para lograr una gestión rápida y ordenada de incidentes de seguridad de la información. (ver cuadro 17)

Cuadro 17. Gestión de incidentes de seguridad de la información.

A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio			**Estado**
A.17.1 Continuidad de seguridad de la información			
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.			
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.	NC
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.	NC
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 implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	NC

Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.13 A17 Aspectos de seguridad de la información de la gestión de continuidad de negocio. El objetivo es determinar los requisitos de seguridad de la información y la continuidad de negocio en situaciones adversas que puedan afectar la operación de la compañía, Ofimarcas debe establecer y documentar procedimientos que permitan reestablecer las operaciones luego de que se materialice una amenaza, los colaboradores deben tener claridad en cómo deben actuar y que deben hacer ante diferentes situaciones, el plan de continuidad de negocio debe ser probado, medido y en caso de ser necesario ajustado para su correcta aplicación y ejecución. (ver cuadro 18)

Cuadro 18. Aspectos de seguridad de la información de la gestión de continuidad de negocio.

A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio			Estado
A.17.1 Continuidad de seguridad de la información			
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.			
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.	NC
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.	NC
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 implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	NC
A.17.2 Redundancias			**Estado**
Objetivo: Asegurarse de la disponibilidad de instalaciones de procesamiento de información.			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Control: Control Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	CP

Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.4.14 A18 Cumplimiento. Garantizar el cumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales de seguridad de la información. Ofimarcas debe identificar, documentar y mantener actualizados los requisitos necesarios para dar cumplimiento a los aspectos mencionados. Es responsabilidad de los directores identificar la legislación que aplica a la compañía según el tipo de negocio. (ver cuadro 19)

Cuadro 19. Cumplimiento

A.18 Cumplimiento	Estado
A.18.1 Cumplimiento de requisitos legales y contractuales	
Objetivo: Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	

Cuadro 19 (continuación)

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.	CS
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.	CS
A.18 Cumplimiento			**Estado**
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 legales de reglamentación, contractuales y de negocio.	CP
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.	CP
A.18.1.5	Reglamentación de controles criptográficos	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	CP
A.18.2 Revisiones de seguridad de la información			**Estado**
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.			
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 los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	NC
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.	NC
A.18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.	NC

Fuente: ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

10.5 INFORME DIAGNÓSTICO ACTUAL DE LOS DOMINIOS

Después de realizar la evaluación de cada uno de los controles de los dominios de la norma ISO/IEC 27001:2013, se presenta un informe que muestra el resultado final. Se utilizaron cuatro criterios de evaluación, cumple satisfactoriamente, cumple parcialmente, no cumple y no aplica por la naturaleza del negocio. Para poder identificar el porcentaje de cumplimiento, se asignó los siguientes valores según el nivel de cumplimiento, cumple satisfactoriamente 100%, cumple parcialmente 50%, no cumple 0%, el total de controles que aplican para Ofimarcas por cada dominio representa el 100%, para obtener el porcentaje de cumplimiento actual se multiplico la cantidad de controles de la valoración por su respectivo porcentaje, luego se sumó y se dividió por la cantidad de controles que aplican por cada dominio (ver cuadro 20).

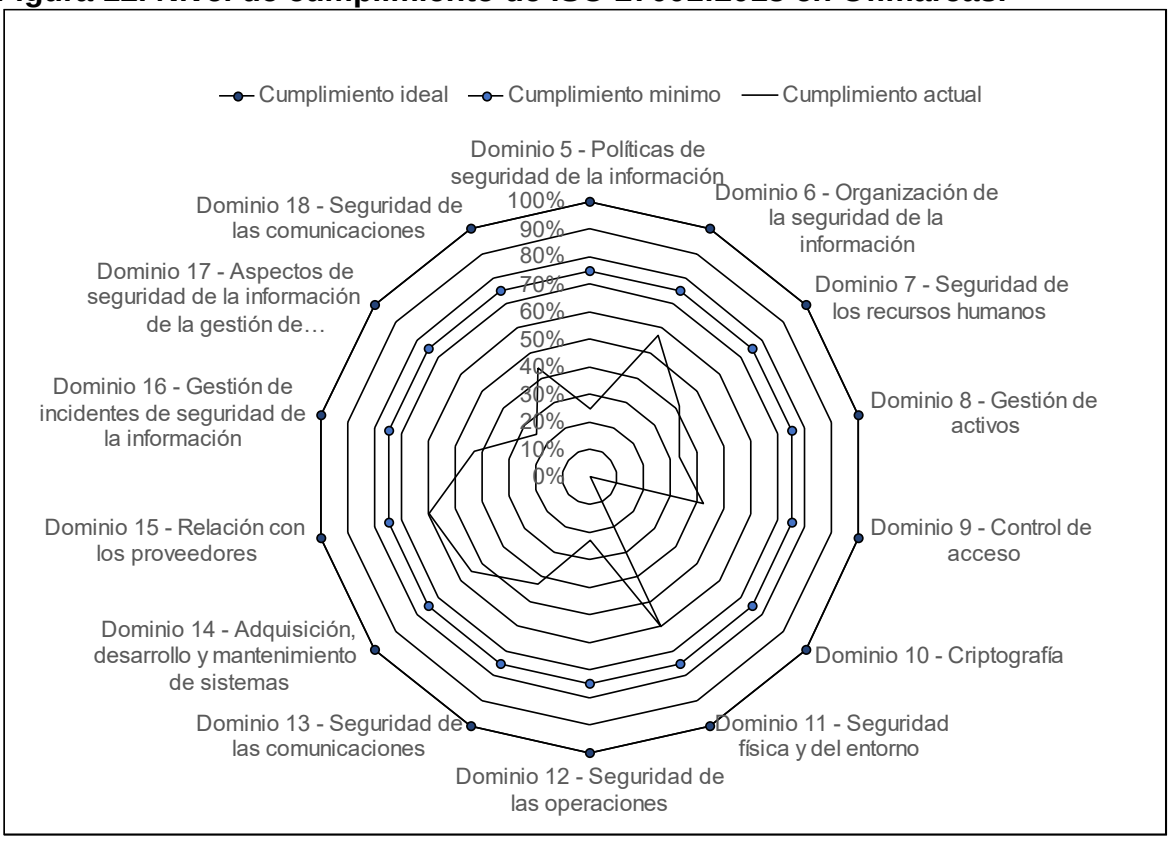
Cuadro 20. Resumen por dominios en Ofimarcas

Dominios de control	Diagnostico						% Cumplimiento	
	Controles que aplican	Satisfactoriamente 100%	Parcialmente 50%	No cumple 0%	No aplica	Cumplimiento actual	Cumplimiento mínimo	Cumplimiento ideal
Dominio 5 - Políticas de seguridad de la información	2	0	1	1	0	25%	75%	100%
Dominio 6 - Organización de la seguridad de la información	7	1	6	2	0	57%	75%	100%
Dominio 7 - Seguridad de los recursos humanos	6	0	5	1	0	42%	75%	100%
Dominio 8 - Gestión de activos	9	0	6	3	1	33%	75%	100%
Dominio 9 - Control de acceso	13	0	11	2	1	42%	75%	100%
Dominio 10 - Criptografía	2	0	0	2	0	0%	75%	100%
Dominio 11 - Seguridad física y del entorno	15	3	12	0	0	60%	75%	100%
Dominio 12 - Seguridad de las operaciones	13	0	6	7	1	23%	75%	100%
Dominio 13 - Seguridad de las comunicaciones	7	0	6	1	0	43%	75%	100%
Dominio 14 - Adquisición, desarrollo y mantenimiento de sistemas	10	4	3	3	3	55%	75%	100%
Dominio 15 - Relación con los proveedores	5	1	4	0	0	60%	75%	100%
Dominio 16 - Gestión de incidentes de seguridad de la información	7	0	6	1	0	43%	75%	100%
Dominio 17 - Aspectos de seguridad de la información de la gestión de continuidad de negocio	4	1	0	3	0	25%	75%	100%
Dominio 18 - Seguridad de las comunicaciones	8	2	3	3	0	44%	75%	100%

Fuente: Autor.

En la figura 12, se muestra el nivel de cumplimiento que tiene Ofimarcas con base a los requisitos de la norma ISO/IEC 27001:2013.

Figura 12. Nivel de cumplimiento de ISO 27001:2013 en Ofimarcas.



Fuente: Autor.

El diagnostico permitió identificar y tener una visual del estado actual de seguridad de la información en Ofimarcas. Se evidencio que su nivel de cumplimiento en los dominios 5- políticas de seguridad de la información, 10 - criptografía, 12 - seguridad en las operaciones y dominio 17 - gestión de la continuidad de negocio, son bajos debido a que no tienen implementados controles o estos no se encuentran debidamente documentados.

11. ACTIVOS DE OFIMARCAS

11.1 IDENTIFICACIÓN, CLASIFICACIÓN Y VALORIZACIÓN DE LOS ACTIVOS DE INFORMACIÓN

La norma ISO 27001:2013 establece que es necesario contar con un inventario de activos de información, en Ofimarcas se identificó los activos de información que intervienen dentro de los procesos de preventa, venta, posventa y soporte. Para realizar la identificación se siguió la guía para la gestión y clasificación de activos de información de Mintic. Se realizó sesiones con los lideres de los procesos, donde se indicó que un activo es todo aquello que le genere valor a la organización. Los campos que se definieron son:

- Código: Identificación de cada activo.
- Nombre del activo: Nombre como se conoce en Ofimarcas.
- Descripción: Detalles y observaciones para su identificación.
- Tipo: Si es un activo físico o virtual.
- Ubicación: Lugar donde se encuentra el activo.
- Estado actual: Descripción de si está en funcionamiento o no.
- Procesos: A los cuales genera valor el activo.

Se definió un formato para realizar el inventario de los activos el cual fue aprobado por los directores y se representa en el cuadro 21.

Cuadro 21. Activos de información Ofimarcas.

Código	Nombre	Descripción	Tipo	Ubicación	Estado actual	Procesos
Ac1	Correo electrónico	Medio de comunicación	Software	Internet	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac2	Computadores	Equipos donde los usuarios realizan sus actividades.	Hardware	Sede Oikos	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac3	ERP contable	(WXMANAGER) Aplicativo HTLM de servicio Técnico,	Software	Internet	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac4	Base de datos (ERP)	Almacenamiento de datos	Software	Internet	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac5	Base de datos (SAPO)	Almacenamiento de datos	Software	Internet	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac6	Impresoras	Equipos de impresión	Hardware	Sede Oikos	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac7	Dominio	Autenticación de los usuarios de Ofimarcas.	Software	Internet	Activo	Preventa - Venta - Posventa - Soporte Técnico

Cuadro 21 (continuación)

Código	Nombre	Descripción	Tipo	Ubicación	Estado actual	Procesos
Ac8	One drive	Medio de almacenamiento definido en Ofimarcas	Software	Internet	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac9	Conexión a internet (ISP)	Medio de comunicación	Servicio	Sede Oikos	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac10	Go do Works Web	Software servicio técnico. (SaaS)	Software	Internet	Activo	Soporte Técnico - Posventa
Ac11	Go do Works Apk	App para soporte técnico	Software	Internet	Activo	Soporte técnico
Ac12	SW Sapo	Generar ordenes de servicio fuera de Bogotá	Software	Internet	Activo	Soporte técnico
Ac13	Switches	Switches de conexión red LAN	Hardware	Sede Oikos	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac14	Router (ISP)	Servicio de internet ETB	Hardware	Sede Oikos	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac15	Firewall (Sophos)	Firewall de la red LAN	Hardware	Sede Oikos	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac16	SW Lector de huellas	Control de acceso	Software	Internet	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac17	Diademas	Dispositivo de comunicación	Hardware	Sede Oikos	Activo	Preventa - Venta - Posventa
Ac18	Móviles Android	Móviles para ingenieros de soporte y laboratorio	Hardware	Sede Oikos	Activo	Servicio Técnico
Ac19	Antivirus	Protección antimalware	Software	Internet	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac20	Plata telefónica	Central telefónica	Hardware	Sede Oikos	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac21	3CX Softphone	Software de teléfono virtual	Software	Internet	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac22	Página web	Página del dominio Ofimarcas	Software	Internet	Activo	Preventa - Venta - Posventa - Soporte Técnico
Ac23	CRM (control operativo)	Plataforma para cargar, negocios, clientes potenciales.	Software	Internet	Activo	Preventa - venta - postventa
Ac24	Essential PIM	Agenda electrónica	Software	Internet	Activo	Posventa - Servicio técnico.

Fuente: Autor.

11.2 CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN EN OFIMARCAS

Teniendo documentado el inventario de activos de información se realizó un proceso de clasificación de los activos de información con la intención de categorizarlos según el nivel de importancia y criticidad para los procesos de preventa, venta, posventa y soporte técnico que son los que se definieron dentro del alcance del sistema de gestión de seguridad de la información. La actividad de clasificación se definió teniendo en cuenta como el activo puede impactar en tres aspectos:

- Pérdidas económicas.
- Afectación de imagen corporativa.
- Incumplimiento legal.

Durante las sesiones con los lideres de proceso, se plantearon escenarios donde se materializaban amenazas, de esta forma los lideres podían identificar con mayor certeza cuanto podría costar a la compañía la afectación de alguno de los activos, como el activo puede afectar la imagen de la empresa o que sanciones se podrían imponer a Ofimarcas en caso de que se viera afectado el activo. En el cuadro 22 se define los criterios de valoración y el valor cuantitativo.

Cuadro 22. Medición de impacto

Campo de afectación	Criterio	Valoración cuantitativa
Pérdidas económicas	Perdidas hasta $ 2,000,000.00.	1
	Rango de perdidas $ 2,000,001.00 y $ 7,000,000.00.	2
	Rango de perdidas $ 7,000,001.00 y $ 13,000,000.	3
	Rango de perdidas $ 13,000,001.00 y $ 20,000,000.	4
	Pérdidas superiores a $ 20,000,001.	5
Afectación imagen corporativa	Sin afectación de imagen, sin afectación de clientes.	1
	Afectación de imagen corporativa.	2
	Afectación de imagen corporativa y clientes.	3
	Afectación de imagen corporativa y clientes estratégicos.	4
	Afectación de imagen corporativa, perdidas de clientes, sanciones regulatorias y legales.	5
Incumplimiento legal.	Sin afectación legal.	1
	Afectación mínima legal.	2
	Sanciones moderadas sin afectación de patrimonio.	3
	Sanciones regulatorias sin proceso penales.	4
	Sanciones regulatorias, procesos penales, indemnizaciones.	5

Fuente: Ofimarcas.

Para lograr valorar el nivel de criticidad en conjunto con la medición del impacto del cuadro 22, se realizó las preguntas que se muestran en el cuadro 23, que permitió a los lideres valorar con mayor certeza la criticidad del activo en relación con una

posible afectación de los pilares de la seguridad de la información, como lo son la disponibilidad, integridad y confidencialidad.

Cuadro 23. Preguntas para valorar la criticidad de los activos.

Tipo de impacto	Preguntas
Pérdidas económicas.	¿Cuánto serían las pérdidas económicas a Ofimarcas si el activo o la información contenida en él no se encuentra disponible por determinado tiempo, es modificada o accedida por personas no autorizadas?
Afectación imagen corporativa.	¿La imagen corporativa de Ofimarcas se puede ver afectada si el activo o la información contenida en él no se encuentra disponible por determinado tiempo, es modificada o accedida por personas no autorizadas?
Incumplimiento legal.	¿Se podrían generar sanciones legales a Ofimarcas si el activo o la información contenida en él no se encuentra disponible por determinado tiempo, es modificada o accedida por personas no autorizadas?

Fuente: Autor.

11.3 CRITICIDAD DE LOS ACTIVOS DE INFORMACIÓN

Se elaboro una clasificación de los activos de información según su criticidad, en el siguiente cuadro se realizó una valoración cuantitativa de 1 a 5, del nivel de criticidad del activo con relación a la medición del tipo de impacto del cuadro 22, se asignó un porcentaje según el nivel de importancia para los directivos de Ofimarcas. Para el cálculo final, se asignó 50% a impacto económico, 30% impacto de imagen corporativa y 20% a impacto legal. (ver cuadro 24)

Cuadro 24. Valoración del nivel de criticidad de los activos en Ofimarcas.

Id	Nombre	Pilares de la seguridad	Pérdidas económicas	Afectación de imagen corporativa	Incumplimiento legal	%	%	%	Total
			50%	30%	20%				
Ac1	Correo electrónico	Disponibilidad	5	5	1	2.5	1.5	0.2	4.2
		Confidencialidad	3	2	1	1.5	0.6	0.2	2.3
		Integridad	3	3	1	1.5	0.9	0.2	2.6
Ac2	Computadores	Disponibilidad	5	3	2	2.5	0.9	0.4	3.8
		Confidencialidad	3	3	3	1.5	0.9	0.6	3
		Integridad	3	3	2	1.5	0.9	0.4	2.8
Ac3	SW ERP contable	Disponibilidad	5	4	2	2.5	1.2	0.4	4.1
		Confidencialidad	4	3	3	2	0.9	0.6	3.5
		Integridad	5	5	5	2.5	1.5	1	5
Ac4	Base de datos (ERP)	Disponibilidad	5	4	2	2.5	1.2	0.4	4.1
		Confidencialidad	4	3	3	2	0.9	0.6	3.5
		Integridad	5	5	5	2.5	1.5	1	5
Ac5	Base de datos (SAPO)	Disponibilidad	5	4	1	2.5	1.2	0.2	3.9
		Confidencialidad	3	3	1	1.5	0.9	0.2	2.6
		Integridad	3	3	2	1.5	0.9	0.4	2.8

Cuadro 24 (continuación)

Id	Nombre	Pilares de la seguridad	Pérdidas económicas	Afectación de imagen corporativa	Incumplimiento legal	%	%	%	Total
Ac6	Impresoras	Disponibilidad	1	1	1	0.5	0.3	0.2	1
		Confidencialidad	1	1	1	0.5	0.3	0.2	1
		Integridad	1	1	1	0.5	0.3	0.2	1
Ac7	Dominio	Disponibilidad	5	5	1	2.5	1.5	0.2	4.2
		Confidencialidad	5	5	1	2.5	1.5	0.2	4.2
		Integridad	5	5	1	2.5	1.5	0.2	4.2
Ac8	One drive	Disponibilidad	5	5	1	2.5	1.5	0.2	4.2
		Confidencialidad	4	3	1	2	0.9	0.2	3.1
		Integridad	5	2	2	2.5	0.6	0.4	3.5
Ac9	Conexión a internet (ISP)	Disponibilidad	5	5	5	2.5	1.5	1	5
		Confidencialidad	2	2	1	1	0.6	0.2	1.8
		Integridad	2	2	1	1	0.6	0.2	1.8
Ac10	Go do Works Web	Disponibilidad	4	3	1	2	0.9	0.2	3.1
		Confidencialidad	2	2	1	1	0.6	0.2	1.8
		Integridad	2	2	1	1	0.6	0.2	1.8
c11	Go do Works Apk	Disponibilidad	3	3	1	1.5	0.9	0.2	2.6
		Confidencialidad	2	2	1	1	0.6	0.2	1.8
		Integridad	2	2	1	1	0.6	0.2	1.8
Ac12	SW Sapo	Disponibilidad	3	3	1	1.5	0.9	0.2	2.6
		Confidencialidad	2	2	1	1	0.6	0.2	1.8
		Integridad	2	2	1	1	0.6	0.2	1.8
Ac13	Switches	Disponibilidad	5	5	1	2.5	1.5	0.2	4.2
		Confidencialidad	5	5	1	2.5	1.5	0.2	4.2
		Integridad	5	5	1	2.5	1.5	0.2	4.2
Ac14	router (ISP)	Disponibilidad	5	5	5	2.5	1.5	1	5
		Confidencialidad	5	4	4	2.5	1.2	0.8	4.5
		Integridad	2	2	1	1	0.6	0.2	1.8
Ac15	Firewall (Sophos)	Disponibilidad	5	5	1	2.5	1.5	0.2	4.2
		Confidencialidad	5	5	1	2.5	1.5	0.2	4.2
		Integridad	5	5	1	2.5	1.5	0.2	4.2
Ac16	SW Lector de huellas	Disponibilidad	3	2	1	1.5	0.6	0.2	2.3
		Confidencialidad	3	2	2	1.5	0.6	0.4	2.5
		Integridad	2	2	2	1	0.6	0.4	2
Ac17	Diademas	Disponibilidad	3	1	1	1.5	0.3	0.2	2
		Confidencialidad	1	1	1	0.5	0.3	0.2	1
		Integridad	1	1	1	0.5	0.3	0.2	1
Ac18	Móviles Android	Disponibilidad	5	4	1	2.5	1.2	0.2	3.9
		Confidencialidad	4	3	1	2	0.9	0.2	3.1
		Integridad	4	3	1	2	0.9	0.2	3.1
Ac19	Consola Antivirus	Disponibilidad	5	4	1	2.5	1.2	0.2	3.9
		Confidencialidad	5	4	1	2.5	1.2	0.2	3.9
		Integridad	5	4	1	2.5	1.2	0.2	3.9
Ac20	Plata telefónica	Disponibilidad	5	5	3	2.5	1.5	0.6	4.6
		Confidencialidad	5	5	5	2.5	1.5	1	5
		Integridad	5	4	5	2.5	1.2	1	4.7
Ac21	3CX Softphone	Disponibilidad	5	4	1	2.5	1.2	0.2	3.9
		Confidencialidad	4	3	3	2	0.9	0.6	3.5

Cuadro 24 (continuación)

Id	Nombre	Pilares de la seguridad	Pérdidas económicas	Afectación de imagen corporativa	Incumplimiento legal	%	%	%	Total
		Integridad	3	3	1	1.5	0.9	0.2	2.6
Ac22	Página web	Disponibilidad	5	5	3	2.5	1.5	0.6	4.6
		Confidencialidad	5	5	5	2.5	1.5	1	5
		Integridad	5	5	5	2.5	1.5	1	5
Ac23	SW CRM (control operativo)	Disponibilidad	5	4	1	2.5	1.2	0.2	3.9
		Confidencialidad	5	2	1	2.5	0.6	0.2	3.3
		Integridad	5	3	1	2.5	0.9	0.2	3.6
Ac24	Essential PIM	Disponibilidad	5	3	1	2.5	0.9	0.2	3.6
		Confidencialidad	3	3	1	1.5	0.9	0.2	2.6
		Integridad	5	3	1	2.5	0.9	0.2	3.6

Fuente: Autor.

11.4 IDENTIFICACIÓN DE ACTIVOS CRÍTICOS

Para realizar un análisis de riesgo con un mayor impacto y objetividad, se debe seleccionar los activos de información que según su valoración son más críticos para los procesos de Ofimarcas y el cumplimiento de sus objetivos de negocio.

En Ofimarcas se definió un sistema de clasificación que tiene en cuenta el mayor valor de impacto sobre cualquiera de los pilares de la seguridad de la información, en el cuadro sistema de selección de activos, están definidos los niveles de criticidad con rangos y escala de colores que se utilizó para la clasificación. (ver cuadro 25)

Cuadro 25. Sistema de selección de activos.

Nivel de criticidad	Rangos de criticidad	Escala de color
Alta	4.1 - 5	Rojo
Media	2.6 - 4	Amarillo
Baja	1 -2.5	Verde

Fuente: Autor.

Con base a los rangos de criticidad que se muestra en el cuadro 25, los activos seleccionados para la gestión de riesgos están resaltados en rojo y amarillo, estos son los activos que mayor impacto pueden ocasionar a Ofimarcas en un escenario en el que se afecte cualquiera de los pilares de la seguridad de la información, la selección se hizo teniendo en cuenta el mayor nivel de afectación en alguno de los tres pilares de la seguridad de la información, confidencialidad, Integridad y disponibilidad. (ver cuadro 26)

Cuadro 26. Activos seleccionados para la gestión de riesgos.

Id	Nombre	Confidencialidad	Integridad	Disponibilidad	Valoración
Ac1	Correo electrónico	2.3	2.6	4.2	4.2
Ac2	Computadores	3	2.8	3.8	3.8

Cuadro 26 (continuación)

Id	Nombre	Confidencialidad	Integridad	Disponibilidad	Valoración
Ac3	SW ERP contable	3.5	5	4.1	5
Ac4	Base de datos (ERP)	3.5	5	4.1	5
Ac5	Base de datos (SAPO)	2.6	2.8	3.9	3.9
Ac6	Impresoras	1	1	1	1
Ac7	Dominio	4.2	4.2	4.2	4.2
Ac8	One drive	3.1	3.5	4.2	4.2
Ac9	Conexión a internet (ISP)	1.8	1.8	5	5
Ac10	Go do Works Web	1.8	1.8	3.1	3.1
Ac11	Go do Works Apk	1.8	1.8	2.6	2.6
Ac12	SW Sapo	1.8	1.8	2.6	2.6
Ac13	Switches	4.2	4.2	4.2	4.2
Ac14	router (ISP)	4.5	1.8	5	5
Ac15	Firewall (Sophos)	4.2	4.2	4.2	4.2
Ac16	SW Lector de huellas	2.5	2	2.3	2.5
Ac17	Diademas	1	1	2	2
Ac18	Móviles Android	3.1	3.1	3.9	3.9
Ac19	Consola Antivirus	3.9	3.9	3.9	3.9
Ac20	Plata telefónica	5	4.7	4.6	5
Ac21	3CX Softphone	3.5	2.6	3.9	3.9
Ac22	Página web	5	5	4.6	5
Ac23	SW CRM (control operativo)	3.3	3.6	3.9	3.9
Ac24	Essential PIM	2.6	3.6	3.6	3.6

Fuente: Autor.

11.5 IDENTIFICACIÓN DE AMENAZAS PARA LA SEGURIDAD DE LA INFORMACIÓN

Los activos de información están expuestos a amenazas de tipo internas y externas, estas pueden afectar cualquier de los tres pilares de la seguridad de la información y son de origen natural o humano, así como pueden darse de forma deliberada o accidental. En Ofimarcas se generó un cuadro con las amenazas que podrían materializarse y el pilar de la seguridad de la información que se podría ver afectado.

Las amenazas se plantearon en conjunto con los lideres de procesos, algunas de ellas ya se habían presentado con anterioridad o se tenía incertidumbre en que pudieran presentarse en un tiempo determinado, en el siguiente cuadro se describe la amenaza y el pilar de seguridad de la información que podría verse impactado.

Cuadro 27. Lista de amenazas de seguridad de la información.

Id	Amenazas	Confidencialidad	Disponibilidad	Integridad
A1	Acceso no autorizado	X	X	
A2	Falla de fluido eléctrico		X	X
A3	Daño físico		X	X
A4	Falla lógica		X	X

Cuadro 27 (continuación)

Id	Amenazas	Confidencialidad	Disponibilidad	Integridad
A5	Denegación de servicio		X	
A6	Eliminación de la Información		X	
A7	Errores de mantenimiento		X	X
A8	Error en configuración	X	X	X
A9	Fallo de servicio de comunicaciones		X	X
A10	Fuga de información	X		
A11	Ingeniería social.	X	X	X
A12	Interceptación de información	X		X
A13	Interceptación de trafico	X	X	X
A14	Interrupción de servicios		X	
A15	Modificación errada de la información	X	X	X
A16	Perdida de dispositivos	X	X	X
A17	Indisponibilidad de la aplicación		X	
A18	Abuso de privilegios	X	X	X
A19	Manipulación errada de equipos	X	X	X

Fuente: MinTIC. Ministerio de Tecnologías de la Información y Comunicaciones. Guía No. 2. Elaboración de la política general de seguridad y privacidad de la información. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>

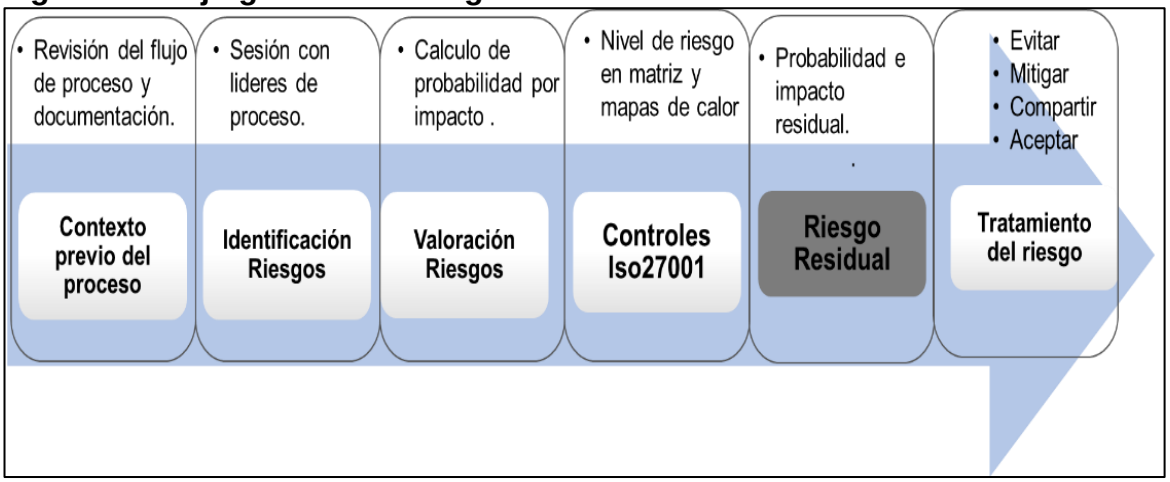
12. ANÁLISIS DE RIESGOS PARA LOS ACTIVOS CRÍTICOS DE OFIMARCAS

El análisis de riesgos está enfocado identificar el nivel de riesgo al que está expuesto un activo de información frente a una amenaza, el riesgo puede verse desde la incertidumbre en cuanto al cumplimiento de los objetivos del negocio. Para Ofimarcas el riesgo es la incertidumbre sobre la protección de la confidencialidad, integridad y disponibilidad de los activos estratégicos de los procesos de preventa, venta, posventa y soporte técnico. Para realizar el cálculo de nivel de riesgo, se utilizó una técnica que se basa en multiplicar la probabilidad por el impacto y de esta forma se obtiene el nivel de riesgo.

12.1 METODOLOGÍA

Para la gestión de riesgos se utilizó como referencia algunas técnicas que se establecen en la norma ISO 31010, en la figura 13 se muestra el flujo de trabajo que se realizó para la identificación, valoración y propuesta de tratamiento a los riesgos en Ofimarcas.

Figura 13.Flujo gestión de riesgos Ofimarcas.



Fuente: Autor.

12.2 PROBABILIDAD

Se entiende como la posibilidad de materialización de un riesgo y puede ser medida con criterios de frecuencia o la facilidad de que se presente teniendo en cuenta factores internos y externos. En Ofimarcas se definió el cuadro de valoración de probabilidad que permite valorar la probabilidad de ocurrencia de una amenaza con su respectivo valor cualitativo y cuantitativo, esta información se observa en el cuadro 28.

Cuadro 28. Valoración de probabilidad.

Probabilidad de ocurrencia	Frecuencia	Valor cualitativo	Valor cuantitativo
El evento podría presentarse en situaciones poco comunes.	12 meses	Improbable	1
Hay una posibilidad leve de que el evento se presente.	6 meses	Poco probable	2
El evento se puede presentar en algún momento.	3 meses	Posible	3
Se espera que el evento se presente varias veces al año.	1 mes	probable	4
Es posible que se presente en la mayoría de las ocasiones.	Mas de 1 vez al mes	Muy probable	5

Fuente: Autor.

12.3 IMPACTO

Se entiende como las consecuencias que podría ocasionar a una compañía la materialización de un riesgo, en Ofimarcas se definió el cuadro 29 valoración de impacto, para estimar el impacto que podría generar la materialización de las amenazas previamente definidas, se determinó una valoración cualitativa realizando una estimación en el impacto económico que podría causar con su respectivo valor cuantitativo.

Cuadro 29. Valoración de impacto.

Impacto	Impacto económico cualitativo	Valor cuantitativo
Insignificante	Pérdidas económicas leves de hasta 2.000.000 millones de pesos.	1
Menor	Pérdidas económicas pequeñas entre $2.000.0001 hasta $7.000.000 de pesos.	2
Moderado	Pérdidas económicas moderadas entre $7,000,001.00 y $ 13,000,000 de pesos.	3
Grave	Pérdidas económicas graves entre $13,000,001.00 y $ 20,000,000 de pesos.	4
Catastrófico	Pérdidas financieras criticas superiores a $ 20,000,001 de pesos.	5

Fuente: Autor.

12.4 VALORACIÓN DE RIESGOS

Para la valoración de los riesgos se estableció el siguiente cuadro donde se define el tipo de riesgo, valor del nivel de riesgo con base probabilidad por el impacto y la acción que se debe realizar para ese nivel de riesgo según el apetito de riesgo aceptado por Ofimarcas.

Cuadro 30. Valoración de los riesgos y criterios de aceptación.

		PROBABILIDAD				
IMPACTO	5	M	M	A	E	E
	4	B	M	M	A	E
	3	B	M	M	M	A
	2	I	B	M	M	M
	1	I	I	B	B	M
		1	2	3	4	5
I: Zona de riesgo inusual		Se puede asumir el riesgo y realizar seguimiento.				
B: Zona de riesgo bajo		Se puede asumir el riesgo y realizar seguimiento.				
M: Zona riesgo medio		Se puede asumir el riesgo mientras se buscan controles que lo reduzcan.				
A: Zona riesgo alto		Se debe reducir el riesgo, evitarlo, compartirlo o transferirlo				
E: Zona riesgo extremo		Se debe reducir el riesgo, evitarlo, compartirlo o transferirlo				

Fuente: Autor

12.5 MAPAS DE CALOR

El nivel de riesgo se obtiene al multiplicar el valor cuantitativo de la probabilidad por el valor cuantitativo del impacto, de esta forma se ubica en el mapa de calor que se definió en Ofimarcas para los activos críticos, para este ejercicio se realizó sesiones con los lideres de los procesos, donde se exponía cada una de las amenazas y en conjunto se determinó el valor para probabilidad e impacto. (ver cuadro 31)

En Ofimarcas se definió una plantilla para realizar la identificación de los riesgos, para cada uno de los activos de información críticos, el cual se muestra a continuación. El objetivo de la matriz de riesgos es contar con un inventario de los activos, las amenazas a las que está expuesto y el nivel de riesgos, también se conoce como catálogo de riesgos de seguridad de la información y sus campos se describieron así:

- Id riesgo: Identificación del riesgo dentro de la plantilla.
- Id activo: Identificación del activo en el inventario de activos.
- Activo: Nombre del activo.
- Amenaza: Definidas en el catálogo de amenazas de MinTic.
- Probabilidad: Valor cuantitativo de la posibilidad de ocurrencia.
- impacto: Valor cuantitativo de la afectación que puede generar.
- Nivel de riesgo: Riesgo inherente sin la aplicación de controles.

Cuadro 31 Identificación y valoración de riesgo inherente.

Id riesgo	Id activo	Activo	Amenaza	Probabilidad	Impacto	Nivel de riesgo
Ac3 - R1	Ac3	SW ERP Contable	Acceso no autorizado	2	2	Riesgo bajo (4)
Ac3 - R2			Indisponibilidad de la aplicación	3	4	Riesgo medio (12)
Ac3 - R3			Eliminación de información	1	4	Riesgo bajo (4)
Ac3 - R4			Fuga de información	2	4	Riesgo medio (8)
Ac3 - R5			Modificación errada de la información	2	5	Riesgo medio (10)

Cuadro 31 (Continuación)

Id riesgo	Id activo	Activo	Amenaza	Probabilidad	Impacto	Nivel de riesgo
Ac3 - R6			Manipulación errada de equipos	2	5	Riesgo medio (10)
Ac3 - R7			Abuso de privilegios	2	5	Riesgo medio (10)
Ac4 - R1	Ac4	Base de datos (ERP)	Acceso no autorizado	1	4	Riesgo bajo (4)
Ac4 - R2			Fuga de información	2	4	Riesgo medio (8)
Ac4 - R3			Eliminación de información	3	5	Riesgo alto (15)
Ac4 - R4			Modificación de la información	3	5	Riesgo alto (15)
Ac4 - R5			Manipulación errada de equipos	2	5	Riesgo medio (10)
Ac9 - R1	Ac9	Conexión a internet (ISP)	Interrupción de servicios	2	5	Riesgo medio (10)
Ac14 - R1	Ac14	Router (ISP)	Acceso no autorizado	2	5	Riesgo medio (10)
Ac14 - R2			Interrupción de servicio eléctrico	4	5	Riesgo extremo (20)
Ac14 - R3			Daño físico	2	5	Riesgo medio (10)
Ac14 - R4			Error en configuración	2	5	Riesgo medio (10)
Ac14 - R5			Manipulación errada de equipos	2	5	Riesgo medio (10)
Ac14 - R6			Interrupción de servicio	2	5	Riesgo medio (10)
Ac22 - R1	Ac22	Página web	Acceso no autorizado	2	5	Riesgo medio (10)
Ac22 - R2			Denegación de servicio	2	5	Riesgo medio (10)
Ac22 - R3			Modificación errada de la información	2	5	Riesgo medio (10)
Ac1 - R1	Ac1	Correo electrónico	Ingeniería social	2	4	Riesgo medio (8)
Ac1 - R2			Fuga de información	2	4	Riesgo medio (8)
Ac1 - R3			Acceso no autorizado	3	5	Riesgo alto (15)
Ac1 - R4			Interceptación de información	1	3	Riesgo bajo (3)
Ac7 - R1	Ac7	Dominio	Acceso no autorizado	2	5	Riesgo medio (10)
Ac7 - R2			Fuga de información	3	5	Riesgo alto (15)
Ac7 - R3			Falla lógica	2	5	Riesgo medio (10)
Ac8 - R1	Ac8	One drive	Acceso no autorizado	2	4	Riesgo medio (8)
Ac8 - R2			Fuga de información	2	4	Riesgo medio (8)
Ac8 - R3			Eliminación de información	3	5	Riesgo alto (15)
Ac8 - R4			Modificación errada de la información	3	5	Riesgo alto (15)
Ac20 - R1	Ac20	Planta telefónica	Acceso no autorizado	2	4	Riesgo medio (8)
Ac20 - R2			Interrupción de servicio eléctrico	4	5	Riesgo extremo (20)
Ac20 - R3			Eliminación de información	2	5	Riesgo medio (10)

Cuadro 31 (continuación)

Id riesgo	Id activo	Activo	Amenaza	Probabilidad	Impacto	Nivel de riesgo
Ac20 - R4			Daño físico	2	4	Riesgo medio (8)
Ac20 - R5			Falla lógica	1	4	Riesgo bajo (4)
Ac20 - R6			Error en mantenimiento	1	4	Riesgo bajo (4)
Ac20 - R7			Manipulación errada de equipos	2	5	Riesgo medio (10)
Ac15 - R1	Ac15	Firewall (Sophos)	Acceso no autorizado	2	5	Riesgo medio (10)
Ac15 - R2			Daño físico	2	5	Riesgo medio (10)
Ac15 - R3			Interrupción de servicio eléctrico	4	5	Riesgo extremo (20)
Ac15 - R4			Perdida del equipo	2	5	Riesgo medio (10)
Ac15 - R5			Eliminación de información	2	5	Riesgo medio (10)
Ac15 - R6			Error en configuración	2	5	Riesgo medio (10)
Ac21 - R1	Ac21	3CX Softphone	Ingeniería social	2	4	Riesgo medio (8)
Ac21 - R2			Interceptación de información	1	5	Riesgo medio (5)
Ac21 - R3			Indisponibilidad de la aplicación	3	4	Riesgo medio (12)
Ac5 - R1	Ac5	Base de datos (SAPO)	Fuga de información	2	3	Riesgo medio (6)
Ac5 - R2			Acceso no autorizado	2	3	Riesgo medio (6)
Ac5 - R3			Eliminación de información	2	5	Riesgo medio (10)
Ac5 - R4			Modificación errada de la información	2	5	Riesgo medio (10)
Ac13 - R1	Ac13	Switches	Acceso no autorizado	2	5	Riesgo medio (10)
Ac13 - R2			Daño físico	2	5	Riesgo medio (10)
Ac13 - R3			Interrupción de servicio eléctrico	4	5	Riesgo extremo (20)
Ac13 - R4			Perdida del equipo	2	5	Riesgo medio (10)
Ac13 - R5			Manipulación errada de equipos	2	5	Riesgo medio (10)
Ac2 - R1	Ac2	Computadores	Acceso no autorizado	4	4	Riesgo alto (16)
Ac2 - R2			Interrupción de servicio eléctrico	4	5	Riesgo extremo (20)
Ac2 - R3			Perdida de equipo	2	5	Riesgo medio (10)
Ac2 - R4			Daño físico	2	3	Riesgo medio (6)
Ac2 - R5			Manipulación errada de equipos	2	5	Riesgo medio (10)
Ac23 - R1	Ac23	SW CRM (control operativo)	Acceso no autorizado	3	4	Riesgo medio (12)
Ac23 - R2			Indisponibilidad de la aplicación	1	4	Riesgo bajo (4)
Ac23 - R3			Denegación de servicio	2	3	Riesgo medio (6)
Ac10 - R1	Ac10	Go do Works Web	Acceso no autorizado	2	3	Riesgo medio (6)

Cuadro 31 (Continuación)

Id riesgo	Id activo	Activo	Amenaza	Probabilidad	Impacto	Nivel de riesgo
Ac10 - R2			Indisponibilidad de la aplicación	1	3	Riesgo bajo (3)
Ac10 - R3			Fuga de información	2	3	Riesgo medio (6)
Ac10 - R4			Denegación de servicio	2	3	Riesgo medio (6)
Ac18 - R1	Ac18	Móviles Android	Ingeniería social	2	4	Riesgo medio (8)
Ac18 - R2			Perdida del dispositivo	3	4	Riesgo medio (12)
Ac18 - R3			Acceso no autorizado	4	3	Riesgo medio (12)
Ac19 - R1	Ac19	Consola Antivirus	Acceso no autorizado	2	5	Riesgo medio (10)
Ac19 - R2			Indisponibilidad de la aplicación	2	5	Riesgo medio (10)
Ac19 - R3			Error en configuración	2	5	Riesgo medio (10)
Ac11 - R1	Ac11	Go do Works Apk	Acceso no autorizado	4	3	Riesgo medio (12)
Ac11 - R2			Indisponibilidad de la aplicación	3	3	Riesgo medio (9)
Ac11 - R3			Fuga de información	4	3	Riesgo medio (12)
Ac12 - R1	Ac12	SW Sapo	Acceso no autorizado	2	2	Riesgo bajo (4)
Ac12 - R2			Indisponibilidad de la aplicación	2	3	Riesgo medio (6)
Ac12 - R3			Fuga de información	2	1	Riesgo inusual (2)
Ac24 - R1	Ac24	SW Essential PIM	Acceso no autorizado	2	2	Riesgo bajo (4)
Ac24 - R2			Indisponibilidad de la aplicación	3	4	Riesgo medio (12)
Ac24 - R3			Fuga de información	2	2	Riesgo bajo (4)

Fuente: Autor

En este punto con base a la probabilidad por el impacto se logra obtener un nivel de riesgo inherente, que hace referencia al riesgo sin la aplicación de controles, y según los criterios de aceptación definidos en Ofimarcas, los riesgos que se trataron son los que están en un nivel alto y extremo, los riesgos en nivel medio deben ser monitoreados mientras se identifican los controles adecuados, para facilitar la interpretación de la información, se utilizó una escala de colores.

13. TRATAMIENTO DE LOS RIESGOS

Del resultado del análisis de riesgos se logró evidenciar aquellos que están en un nivel de riesgo no aceptable. La estrategia que se definió en Ofimarcas para estos riesgos, consistió en aplicar los controles del anexo A de la norma ISO27001.

13.1 VALORACIÓN DE CONTROLES

Para el tratamiento de los riesgos alto y extremos identificados en el proceso anterior, se definieron los controles del anexo A de la norma ISO/IEC 27001:2013, de acuerdo con los criterios de aceptación que se muestran en el siguiente cuadro, con la intención de reducir la probabilidad o el impacto de estos.

Cuadro 32. Valoración de los riesgos y criterios de aceptación.

I: Zona de riesgo	Se puede asumir el riesgo y realizar seguimiento.
B: Zona de riesgo	Se puede asumir el riesgo y realizar seguimiento.
M: Zona riesgo medio	Se puede asumir el riesgo mientras se buscan controles que lo reduzcan.
A: Zona riesgo alto	Se debe reducir el riesgo, evitarlo, compartirlo o transferirlo
E: Zona riesgo	Se debe reducir el riesgo, evitarlo, compartirlo o transferirlo

Fuente: Autor

Teniendo como base los riesgos que no son aceptables por Ofimarcas, se realizó la asignación de cada uno de los controles que aplica para las amenazas descritas anteriormente, de esta forma se realiza el tratamiento de los riesgos que no son aceptables buscando reducir la probabilidad o el impacto de riesgos, generando así el riesgo residual.

Cuadro 33. Lista de controles aplicables para las amenazas.

Id	Amenazas	Código controles Anexo A
A1	Acceso no autorizado	9.2.6 - 9.2.5 - 9.2.4 - 9.2.3 - 9.2.2 - 9.2.1 - 7.2.3 - 7.2.2 - 7.1.2 - 7.1.1 - 5.1.1 - 13.1.3 - 13.1.2 - 13.1.1 - 12.4.4 - 12.4.3 - 12.4.2 - 12.4.1 - 11.2.9 - 11.2.8 - 11.2.6 - 11.2.5 - 11.2.1.
A2	Falla de fluido eléctrico	8.2.3 - 17.1.3 - 17.1.2 - 17.1.1 - 15.1.3 - 15.1.2 - 15.1.1 - 11.1.4 - 11.1.3 - 11.1.2 - 11.1.1.
A3	Daño físico	12.1.1 - 11.2.9 - 11.2.4 - 11.2.2 - 11.2.1 - 11.1.5 - 11.1.3 - 11.1.1 - 11.1.2.
A4	Daño lógico	9.4.4 - 9.4.1 - 8.1.2 - 8.1.1 - 6.1.2 - 14.2.4 - 14.2.3 - 12.7.1 - 12.6.2 - 12.6.1 - 12.4.4 - 12.4.3 - 12.4.2 - 12.3.1 - 12.2.1.
A5	Denegación de servicio	9.1.2 - 9.1.1 - 16.1.6 - 13.1.3 - 13.1.2 - 13.1.1 - 12.6.2 - 12.6.1 - 12.4.4 - 12.4.3 -12.4.1-12.2.1.
A6	Eliminación de la Información	8.2.3 - 8.2.2 - 8.1.3 - 7.2.3 - 7.2.2 - 7.2.1 - 7.1.2 - 7.1.1 - 6.1.1 - 5.1.1- 12.4.2 - 12.4.1-12.3.1.
A7	Errores de mantenimiento	8.2.3 - 7.2.3 - 7.2.2 - 7.2.1 - 5.1.1 - 12.4.3 - 12.4.1 - 11.2.4 - 11.1.5.
A8	Error en configuración	9.4.1 - 8.2.3 - 8.2.2 - 6.1.2 - 5.1.1 - 14.2.4 - 12.4.2 - 12.4.1 - 12.3.1 - 12.1.2 - 12.1.1.

Cuadro 33 (Continuación)

Id	Amenazas	Código controles Anexo A
A9	Fallo de servicios de comunicaciones	17.1.3 - 17.1.2 - 17.1.1 - 16.1.6 - 15.1.3 - 15.1.1.
A10	Fuga de información	9.4.4 - 9.4.3 - 9.4.2 - 9.4.1 - 9.2.5 - 9.2.4 - 9.2.3 - 9.2.2 - 9.2.1 - 9.1.2 - 9.1.1 - 8.2.3 - 8.2.2 - 8.1.2 - 8.1.1 - 7.3.1 - 7.2.3 - 7.2.2 - 7.2.1 - 7.1.2 - 7.1.1 - 6.2.1 - 5.1.1 - 12.4.2 - 12.2.1 - 11.2.9 - 11.2.8 - 11.2.6 - 11.2.1 - 11.1.3 - 11.1.2 - 10.1.1 - 18.1.1.
A11	Ingeniería social.	7.2.3 - 7.2.2 - 7.2.1 - 6.1.4 - 5.1.2 - 5.1.1 - 16.1.6 - 16.1.4 - 16.1.3 - 16.1.2 - 13.1.2 - 13.1.1 - 12.6.2 - 12.6.1 - 12.2.1 - 11.1.3 - 11.1.2.
A12	Interceptación de información	13.1.3 - 13.1.2 - 13.1.1 - 12.6.2 - 12.6.1 - 12.2.1 - 11.2.6 - 11.2.5 - 11.1.2 - 10.1.1.
A13	Interceptación de trafico	9.4.1 - 13.1.3 - 13.1.2 - 13.1.1 - 12.7.1 - 2.6.2 - 12.6.1 - 2.4.2 -2.4.1.
A14	Interrupción de servicios	17.1.3 - 17.1.2 - 17.1.1 - 16.1.5 - 16.1.2 - 15.2.2 - 15.2.1 - 15.1.3 - 15.1.2 - 15.1.1.
A15	Modificación erada de la información	9.4.2 - 9.4.1 - 9.1.2 - 9.1.1 - 8.2.3 - 8.2.2- 8.2.1- 7.1.2- 5.1.1- 2.4.2 -2.3.1.
A16	Perdida de dispositivos	5.1.1 - 18.1.4 - 17.2.1 - 17.1.3 - 17.1.2 - 17.1.1 - 16.1.5 - 11.2.8 - 11.2.6 - 11.2.5 - 11.1.5 - 11.1.4 - 11.1.2 - 11.1.1 - 10.1.1.
A17	Indisponibilidad de la aplicación	17.1.3 - 17.1.2 - 17.1.1 - 16.1.6 - 16.1.5 - 16.1.2 - 15.1.3.
A18	Abuso de privilegios	9.2.6 - 9.2.3 - 9.2.2 - 9.1.2 - 9.1.1 - 16.1.6 - 12.4.4 - 12.4.3 - 12.4.2.
A19	Manipulación errada de equipos	6.1.2 - 12.4.2 - 12.4.1 - 12.1.3 - 12.1.2 - 12.1.1 - 11.2.9 - 11.2.4 - 11.2.3 - 11.2.2 - 11.2.1.

Fuente: Autor

13.2 EFECTIVIDAD DE CONTROLES

Teniendo en cuenta los controles que se identificaron en el anexo A de la norma ISO/IEC 27001:2013, se procede a valorar la efectividad de los controles (ver cuadro 34) en cuanto el nivel de impacto y/o probabilidad al momento de ser aplicados, el objetivo es analizar que efecto tiene aplicar el control al riesgo, teniendo en cuenta que existen diferentes tipos de controles:

- Preventivos: Anticipan eventos no deseados antes de que sucedan.

- Detectivos: Identifican un evento en el momento en el que está ocurriendo.

- Correctivos: Aseguran que las medidas correctivas sean tomadas con la intención de revertir un evento no deseado.

Cuadro 34 Efectividad controles.

Reducción en probabilidad		Reducción en Impacto	
Efectivo	2	**Alto**	2
Aceptable	1	**Medio**	1
Incierto	0	**Bajo**	0

Fuente: Autor

13.2.1 Efectividad del control frente a la probabilidad.

- Efectivo: Cumple casi en su totalidad el objetivo.
- Aceptable: Cumple parcialmente.
- Incierto: No se tiene precisión en cuanto al cumplimiento.

13.2.2 Efectividad del control frente al impacto.

- Alto: Se reduce casi en su totalidad el impacto generado.
- Medio: Se reduce parcialmente el impacto que ocasiona la amenaza.
- Bajo: El control no impide la materialización de la amenaza.

Del cuadro 35 al 52 se puede ver la valoración de los controles que aplican para mitigar la probabilidad o el impacto de la materialización de las amenazas que se identificaron en Ofimarcas.

Cuadro 35. Valoración de controles para falla fluido eléctrico

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A2	Falla de fluido eléctrico	8.2.3	Manipulación de activos.	1	2
		17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	2	2
		17.1.2	Implantación de la continuidad de la seguridad de la información.	2	2
		17.1.1	Planificación de la continuidad de la seguridad de la información.	2	2
		15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	2	2
		15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	1	2
		15.1.1	Política de seguridad de la información para suministradores.	1	2
		11.1.4	Protección contra las amenazas externas y ambientales.	1	2
		11.1.3	Seguridad de oficinas, despachos y recursos.	0	2
		11.1.2	Controles físicos de entrada.	0	2
		11.1.1	Perímetro de seguridad física.	0	2

Fuente: Autor

Cuadro 36. Valoración de controles para acceso no autorizado

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A1	Acceso no autorizado	9.2.6	Retirada o adaptación de los derechos de acceso	0	2
		9.2.5	Revisión de los derechos de acceso de los usuarios.	1	2
		9.2.4	Gestión de información confidencial de autenticación de usuarios.	0	2
		9.2.3	Gestión de los derechos de acceso con privilegios especiales.	1	2
		9.2.2	Gestión de los derechos de acceso asignados a usuarios.	1	2
		9.2.1	Gestión de altas/bajas en el registro de usuarios.	0	2
		7.2.3	Proceso disciplinario.	0	1
		7.2.2	Concienciación, educación y capacitación en seguridad de la información	1	2
		7.1.2	Términos y condiciones de contratación.	0	2
		7.1.1	Investigación de antecedentes.	0	1
		5.1.1	Conjunto de políticas para la seguridad de la información.	0	1
		13.1.3	Segregación de redes.	2	2
		13.1.2	Mecanismos de seguridad asociados a servicios en red.	2	1
A1	Acceso no autorizado	13.1.1	Controles de red.	2	2
		12.4.4	Sincronización de relojes.	2	0
		12.4.3	Registros de actividad del administrador y operador del sistema.	2	1
		12.4.2	Protección de los registros de información.	2	1
		12.4.1	Registro y gestión de eventos de actividad.	2	1
		11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	0	2
		11.2.8	Equipo informático de usuario desatendido.	0	2
		11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	0	2
		11.2.5	Salida de activos fuera de las dependencias de la empresa.	0	2
		11.2.1	Emplazamiento y protección de equipos.	0	2

Fuente: Autor

Cuadro 37. Valoración de controles para daño físico.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A3	Daño físico	12.1.1	Documentación de procedimientos de operación.	0	2
		11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	2	2
		11.2.4	Mantenimiento de los equipos.	2	2
		11.2.2	Instalaciones de suministro.	2	2
		11.2.1	Emplazamiento y protección de equipos.	2	2
		11.1.5	El trabajo en áreas seguras.	1	2
		11.1.3	Seguridad de oficinas, despachos y recursos.	1	2
		11.1.1	Perímetro de seguridad física.	1	2
		11.1.2	Controles físicos de entrada.	1	2

Fuente: Autor

Cuadro 38. Valoración de controles para daño lógico.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A4	Daño lógico	9.4.4	Uso de herramientas de administración de sistemas.	1	2
		9.4.1	Restricción del acceso a la información.	2	1
		8.1.2	Propiedad de los activos.	1	0
		8.1.1	Inventario de activos.	1	2
		12.2.1	Controles contra el código malicioso.	1	2
		14.2.4	Restricciones a los cambios en los paquetes de software.	2	1
		14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	2	1
		12.7.1	Controles de auditoría de los sistemas de información.	1	1
		12.6.2	Restricciones en la instalación de software.	1	1
		12.6.1	Gestión de las vulnerabilidades técnicas.	1	1
		12.4.4	Sincronización de relojes.	1	0
		12.4.3	Registros de actividad del administrador y operador del sistema.	1	1
		12.4.2	Protección de los registros de información.	2	0
		12.3.1	Copias de seguridad de la información.	2	2

Fuente: Autor

Cuadro 39. Valoración de controles para denegación de servicio.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A5	Denegación de servicio	9.1.2	Control de acceso a las redes y servicios asociados.	2	1
		9.1.1	Política de control de accesos.	2	2
		16.1.6	Aprendizaje de los incidentes de seguridad de la información.	2	2
		13.1.3	Segregación de redes.	2	1
		13.1.2	Mecanismos de seguridad asociados a servicios en red.	2	1
		13.1.1	Controles de red.	2	1
		12.6.2	Restricciones en la instalación de software.	0	2
		12.6.1	Gestión de las vulnerabilidades técnicas.	2	2
		12.4.4	Sincronización de relojes.	0	2
		12.4.3	Registros de actividad del administrador y operador del sistema.	1	1
		12.4.1	Registro y gestión de eventos de actividad.	1	2
		12.2.1	Controles contra el código malicioso.	1	1

Fuente: Autor

Cuadro 40. Valoración de controles para eliminación de la Información.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A6	Eliminación de la Información	8.2.3	Manipulación de activos.	1	2
		8.2.2	Etiquetado y manipulado de la información.	2	2
		8.1.3	Uso aceptable de los activos.	1	2
		7.2.3	Proceso disciplinario.	1	1
		7.2.2	Concienciación, educación y capacitación en seguridad de la información	1	2
		7.2.1	Responsabilidades de gestión.	1	1
		7.1.2	Términos y condiciones de contratación.	1	2
		7.1.1	Investigación de antecedentes.	1	1
		6.1.1	Asignación de responsabilidades para la seguridad de la información.	1	1
		5.1.1	Conjunto de políticas para la seguridad de la información.	1	2

Cuadro 40 (continuación)

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
		12.4.2	Protección de los registros de información.	2	2
		12.4.1	Registro y gestión de eventos de actividad.	2	1
		12.3.1	Copias de seguridad de la información.	2	1

Fuente: Autor

Cuadro 41. Valoración de controles para errores de mantenimiento.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A7	Errores de mantenimiento	8.2.3	Manipulación de activos.	1	2
		7.2.3	Proceso disciplinario.	0	1
		7.2.2	Concienciación, educación y capacitación en seguridad de la información	1	2
		7.2.1	Responsabilidades de gestión.	1	1
		5.1.1	Conjunto de políticas para la seguridad de la información.	1	1
		12.4.3	Registros de actividad del administrador y operador.	2	2
		12.4.1	Registro de eventos de actividad.	2	1
		11.2.4	Mantenimiento de los equipos.	1	2
		11.1.5	El trabajo en áreas seguras.	1	2

Fuente: Autor

Cuadro 42. Valoración de controles para error en configuración.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A8	Error en configuración	9.4.1	Restricción del acceso a la información.	2	1
		8.2.3	Manipulación de activos.	2	1
		8.2.2	Etiquetado y manipulado de la información.	1	2
		6.1.2	Segregación de tareas.	1	2
		5.1.1	Conjunto de políticas para la seguridad de la información.	0	2
		14.2.4	Restricciones a los cambios en los paquetes de software.	2	2
		12.4.2	Protección de los registros de información.	2	1

Cuadro 42 (Continuación)

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
		12.4.1	Registro y gestión de eventos de actividad.	1	2
		12.3.1	Copias de seguridad de la información.	2	1
		12.1.2	Gestión de cambios.	2	2
		12.1.1	Documentación de procedimientos de operación.	1	2

Fuente: Autor

Cuadro 43. Valoración de controles para fallo de servicios de comunicaciones.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A9	Fallo de servicios de comunicaciones	17.1.3	Verificación y evaluación de la continuidad de la seguridad de la información.	1	2
		17.1.2	Implantación de la continuidad de la seguridad de la información.	1	2
		17.1.1	Planificación de la continuidad de la seguridad de la información.	1	2
		16.1.6	Aprendizaje de los incidentes de seguridad de la información.	2	1
		15.1.3	Cadena de suministro en tic.	1	1
		15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	2	2

Fuente: Autor

Cuadro 44. Valoración de controles para fuga de información.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A10	Fuga de información	9.4.4	Uso de herramientas de administración de sistemas.	1	2
		9.4.3	Gestión de contraseñas de usuario.	1	2
		9.4.2	Procedimientos seguros de inicio de sesión.	1	2
		9.4.1	Restricción del acceso a la información.	2	2
		9.2.5	Revisión de los derechos de acceso de los usuarios.	1	2
		9.2.4	Gestión de información confidencial de autenticación de usuarios.	1	2

Cuadro 44 (Continuación)

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
		9.2.3	Gestión de los derechos de acceso con privilegios especiales.	1	2
		9.2.2	Gestión de los derechos de acceso asignados a usuarios.	1	2
		9.2.1	Gestión de altas/bajas en el registro de usuarios.	1	2
A10	Fuga de información	9.1.2	Control de acceso a las redes y servicios asociados.	1	2
		9.1.1	Política de control de accesos.	0	2
		8.2.3	Manipulación de activos.	0	2
		8.2.2	Etiquetado y manipulado de la información.	0	2
		8.1.2	Propiedad de los activos.	0	2
		8.1.1	Inventario de activos.	0	2
		7.3.1	Cese o cambio de puesto de trabajo.	0	2
		7.2.3	Proceso disciplinario.	1	1
		7.2.2	Concienciación, educación y capacitación en seguridad de la información	0	2
		7.2.1	Responsabilidades de gestión.	0	2
		7.1.2	Términos y condiciones de contratación.	0	2
		7.1.1	Investigación de antecedentes.	0	2
		6.2.1	Política de uso de dispositivos para movilidad.	0	2
		5.1.1	Conjunto de políticas para la seguridad de la información.	1	2
		12.4.2	Protección de los registros de información.	2	1
		12.2.1	Controles contra el código malicioso.	1	2
		11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	1	2
		11.2.8	Equipo informático de usuario desatendido.	1	2
		11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	1	2
		11.2.1	Emplazamiento y protección de equipos.	1	2
		11.1.3	Seguridad de oficinas, despachos y recursos.	1	2
		11.1.2	Controles físicos de entrada.	1	2
		10.1.1	Política de uso de los controles criptográficos.	2	1
		18.1.1	Identificación de la legislación aplicable.	2	2

Fuente: Autor

Cuadro 45. Valoración de controles para ingeniería social.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A11	Ingeniería social.	7.2.3	Proceso disciplinario.	0	2
		7.2.2	Concienciación, educación y capacitación en SI.	1	2
		7.2.1	Responsabilidades de gestión.	1	2
		6.1.4	Contacto con grupos de interés especial.	0	1
		5.1.2	Revisión de las políticas para la seguridad de la información.	0	1
		5.1.1	Conjunto de políticas para la seguridad de la información.	0	2
		16.1.6	Aprendizaje de los incidentes de seguridad de la información.	0	1
		16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	0	2
		16.1.3	Notificación de puntos débiles de la seguridad.	0	2
		16.1.2	Notificación de los eventos de seguridad de la información.	0	2
		13.1.2	Mecanismos de seguridad asociados a servicios en red.	1	2
		13.1.1	Controles de red.	2	1
		12.6.2	Restricciones en la instalación de software.	0	1
		12.6.1	Gestión de las vulnerabilidades técnicas.	2	1
		12.2.1	Controles contra el código malicioso.	2	1
		11.1.3	Seguridad de oficinas, despachos y recursos.	1	1
		11.1.2	Controles físicos de entrada.	1	2

Fuente: Autor

Cuadro 46. Valoración de controles para interceptación de información.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A12	Interceptación de información	13.1.3	Segregación de redes.	2	1
		13.1.2	Mecanismos de seguridad asociados a servicios en red.	2	2
		13.1.1	Controles de red.	2	2

Cuadro 46 (Continuación)

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A12	Interceptación de información	12.6.2	Restricciones en la instalación de software.	1	1
		12.6.1	Gestión de las vulnerabilidades técnicas.	1	1
		12.2.1	Controles contra el código malicioso.	2	2
		11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	2	2
		11.2.5	Salida de activos fuera de las dependencias de la empresa.	2	2
		11.1.2	Controles físicos de entrada.	1	2
		10.1.1	Política de uso de los controles criptográficos.	2	2

Fuente: Autor

Cuadro 47. Valoración de controles para interrupción de servicios.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A14	Interrupción de servicios	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	1	2
		17.1.2	Implantación de la continuidad de la seguridad de la información.	1	2
		17.1.1	Planificación de la continuidad de la SI.	1	2
		16.1.5	Respuesta a los incidentes de seguridad.	1	2
		16.1.2	Notificación de los eventos de seguridad de la información.	1	2
		15.2.2	Gestión de cambios en los servicios prestados por terceros.	1	2
		15.2.1	Supervisión y revisión de los servicios prestados por terceros.	2	2
		15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	2	1
		15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	2	1
		15.1.1	Política de seguridad de la información para suministradores.	2	1

Fuente: Autor

Cuadro 48. Valoración de controles para modificación erada de la información.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A15	Modificación errada de la información	9.4.2	Procedimientos seguros de inicio de sesión.	1	2
		9.4.1	Restricción del acceso a la información.	1	2
		9.1.2	Control de acceso a las redes y servicios asociados.	1	2
		9.1.1	Política de control de accesos.	1	2
		8.2.3	Manipulación de activos.	0	2
		8.2.2	Etiquetado y manipulado de la información.	1	2
		8.2.1	Directrices de clasificación.	0	2
		7.1.2	Términos y condiciones de contratación.	0	2
		5.1.1	Conjunto de políticas para la seguridad de la información.	0	2
		12.4.2	Protección de los registros de información.	2	1
		12.3.1	Copias de seguridad de la información.	2	1

Fuente: Autor

Cuadro 49. Valoración de controles para perdida de dispositivos

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A16	Perdida de dispositivos	5.1.1	Conjunto de políticas para la seguridad de la información.	0	2
		18.1.4	Protección de datos y privacidad de la información personal.	2	1
		17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	2	2
		17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	1	2
		17.1.2	Implantación de la continuidad de la seguridad de la información.	1	2
		17.1.1	Planificación de la continuidad de la seguridad de la información.	1	2
		16.1.5	Respuesta a los incidentes de seguridad.	1	2
		11.2.8	Equipo informático de usuario desatendido.	1	2

Fuente: Autor

Cuadro 49 (continuación).

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A16	Perdida de dispositivos	11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	2	2
		11.2.5	Salida de activos fuera de las dependencias de la empresa.	2	2
		11.1.5	El trabajo en áreas seguras.	1	2
		11.1.4	Protección contra las amenazas externas y ambientales.	2	2
		11.1.2	Controles físicos de entrada.	1	2
		11.1.1	Perímetro de seguridad física.	1	2
		10.1.1	Política de uso de los controles criptográficos.	2	1

Fuente: Autor

Cuadro 50. Valoración de controles para indisponibilidad de la aplicación.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A17	Indisponibilidad de la aplicación	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	1	2
		17.1.2	Implantación de la continuidad de la SI.	2	2
		17.1.1	Planificación de la continuidad de la SI.	1	2
		16.1.6	Aprendizaje de los incidentes de SI.	1	2
		16.1.5	Respuesta a los incidentes de seguridad.	2	2
		16.1.2	Notificación de los eventos de la SI.	2	1
		15.1.3	Cadena de suministro en TIc.	1	1

Fuente: Autor

Cuadro 51. Valoración de controles para abuso de privilegios.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A18	Abuso de privilegios	9.2.6	Retirada o adaptación de los derechos de acceso	1	2
		9.2.3	Gestión de los derechos de acceso con privilegios especiales.	1	2
		9.2.2	Gestión de los derechos de acceso asignados a usuarios.	1	2
		9.1.2	Control de acceso a las redes y servicios asociados.	2	2

Cuadro 51 (Continuación)

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A18	Abuso de privilegios	9.1.1	Política de control de accesos.	1	2
		16.1.6	Aprendizaje de los incidentes de SI.	2	2
		12.4.4	Sincronización de relojes.	1	1
		12.4.3	Registros de actividad del administrador y operador del sistema.	2	1
		12.4.2	Protección de los registros de información.	2	1

Fuente: Autor

Cuadro 52. Valoración de controles para manipulación errada de equipos.

Id	Amenazas	Código	Descripción	Efectividad en Impacto	Efectividad en probabilidad
A19	Manipulación errada de equipos	6.1.2	Segregación de tareas.	1	1
		12.4.2	Protección de los registros de información.	2	1
		12.4.1	Registro y gestión de eventos de actividad.	2	1
		12.1.2	Gestión de cambios.	2	2
		12.1.1	Documentación de procedimientos de operación.	1	2
		11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	1	2
		11.2.4	Mantenimiento de los equipos.	1	2
		11.2.3	Seguridad del cableado.	1	2
		11.2.2	Instalaciones de suministro.	1	1
		11.2.1	Emplazamiento y protección de equipos.	1	2

Fuente: Autor

Para cada una de las amenazas se realizó una selección y valoración de controles y con base al promedio de la efectividad de los controles se procedió a calcular el riesgo residual al restar el valor en 1 o en 2 en el impacto o la probabilidad, como se aprecia en el cuadro 53.

Los controles se aplicaron a cada uno de los riesgos como estrategia del tratamiento, en el cuadro aplicación de controles a los riegos se puede ver la reducción en cuanto a la probabilidad o impacto al aplicar el control, lo que genera una nueva probabilidad y un nuevo impacto, obteniendo así el riesgo residual de acuerdo con los criterios de aceptación de Ofimarcas.

Cuadro 53. Aplicación de controles a los riesgos

Código riesgo	Código activo	Activo	Riesgo	Amenaza	Probabilidad	Impacto	Nivel de riesgo Inherente	Reducción probabilidad	Reducción impacto	Nueva probabilidad	Nuevo impacto	Nivel de riesgo residual
Ac3 - R2	Ac3	SW ERP Contable	R2	Indisponibilidad de la aplicación	3	4	Riesgo medio (12)	2	2	1	2	Riesgo inusual (2)
Ac3 - R4			R4	Fuga de información	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac3 - R5			R5	Modificación errada de la información	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac3 - R6			R6	Manipulación errada de equipos	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac3 - R7			R7	Abuso de privilegios	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac4 - R2	Ac4	Base de datos (ERP)	R2	Fuga de información	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac4 - R3			R3	Eliminación de información	3	5	Riesgo alto (15)	1	2	2	3	Riesgo medio (6)
Ac4 - R4			R4	Modificación de la información	3	5	Riesgo alto (15)	1	2	2	3	Riesgo medio (6)
Ac4 - R5			R5	Manipulación errada de equipos	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac9 - R1	Ac9	Conexión a internet (ISP)	R1	Interrupción de servicios	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)

Fuente: Autor

Cuadro 53 (continuación)

Código riesgo	Código activo	Activo	Riesgo	Amenaza	Probabilidad	Impacto	Nivel de riesgo Inherente	Reducción probabilidad	Reducción impacto	Nueva probabilidad	Nuevo impacto	Nivel de riesgo residual
Ac14 - R1	Ac14	Router (ISP)	R1	Acceso no autorizado	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (4)
Ac14 - R2			R2	Interrupción de servicio eléctrico	4	5	Riesgo extremo (20)	1	2	3	3	Riesgo medio (9)
Ac14 - R3			R3	Daño físico	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac14 - R4			R4	Error en configuración	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac14 - R5			R5	Manipulación errada de equipos	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac14 - R6			R6	Interrupción de servicio de comunicaciones	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac20 - R1	Ac20	Plata telefónica	R1	Acceso no autorizado	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac20 - R2			R2	Interrupción de servicio eléctrico	4	5	Riesgo extremo (20)	1	2	3	3	Riesgo medio (9)
Ac20 - R3			R3	Eliminación de información	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac20 - R4			R4	Daño físico	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac20 - R7			R7	Manipulación errada de equipos	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac22 - R1	Ac22	Página web	R1	Acceso no autorizado	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (4)
Ac22 - R2			R2	Denegación de servicio	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac22 - R3			R3	Modificación errada de la información	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)

Fuente: Autor

Cuadro 53 (continuación).

Código riesgo	Código activo	Activo	Riesgo	Amenaza	Probabilidad	Impacto	Nivel de riesgo Inherente	Reducción probabilidad	Reducción impacto	Nueva probabilidad	Nuevo impacto	Nivel de riesgo residual
Ac1 - R1	Ac1	Correo electrónico	R1	Ingeniería social	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac1 - R2			R2	Fuga de información	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac1 - R3			R3	Acceso no autorizado	3	5	Riesgo alto (15)	1	2	2	3	Riesgo medio (6)
Ac7 - R1	Ac7	Dominio	R1	Acceso no autorizado	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (4)
Ac7 - R2			R2	Fuga de información	3	5	Riesgo alto (15)	1	2	2	3	Riesgo medio (6)
Ac7 - R3			R3	Falla lógica	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac8 - R1	Ac8	One drive	R1	Acceso no autorizado	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac8 - R2			R2	Fuga de información	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac8 - R3			R3	Eliminación de información	3	5	Riesgo alto (15)	1	2	2	3	Riesgo medio (6)
Ac8 - R4			R4	Modificación errada de la información	3	5	Riesgo alto (15)	1	2	2	3	Riesgo medio (6)
Ac15 - R1	Ac15	Firewall (Sophos)	R1	Acceso no autorizado	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (4)
Ac15 - R2			R2	Daño físico	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac15 - R3			R3	Interrupción de servicio eléctrico	4	5	Riesgo extremo (20)	1	2	3	3	Riesgo medio (9)
Ac15 - R4			R4	Perdida del equipo	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac15 - R5			R5	Eliminación de información	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac15 - R6			R6	Error en configuración	2	5	Riesgo medio (10)	1	1	1	4	Riesgo bajo (4)

Fuente: Autor

Cuadro 53 (continuación).

Código riesgo	Código activo	Activo	Riesgo	Amenaza	Probabilidad	Impacto	Nivel de riesgo Inherente	Reducción probabilidad	Reducción impacto	Nueva probabilidad	Nuevo impacto	Nivel de riesgo residual
Ac1 - R1	Ac1	Correo electrónico	R1	Ingeniería social	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac1 - R2			R2	Fuga de información	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac1 - R3			R3	Acceso no autorizado	3	5	Riesgo alto (15)	1	2	2	3	Riesgo medio (6)
Ac7 - R1	Ac7	Dominio	R1	Acceso no autorizado	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (4)
Ac7 - R2			R2	Fuga de información	3	5	Riesgo alto (15)	1	2	2	3	Riesgo medio (6)
Ac7 - R3			R3	Falla lógica	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac8 - R1	Ac8	One drive	R1	Acceso no autorizado	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac8 - R2			R2	Fuga de información	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac8 - R3			R3	Eliminación de información	3	5	Riesgo alto (15)	1	2	2	3	Riesgo medio (6)
Ac8 - R4			R4	Modificación errada de la información	3	5	Riesgo alto (15)	1	2	2	3	Riesgo medio (6)

Fuente: Autor

Cuadro 53 (continuación).

Código riesgo	Código activo	Activo	Riesgo	Amenaza	Probabilidad	Impacto	Nivel de riesgo Inherente	Reducción probabilidad	Reducción impacto	Nueva probabilidad	Nuevo impacto	Nivel de riesgo residual
Ac15 - R1	Ac15	Firewall (Sophos)	R1	Acceso no autorizado	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (4)
Ac15 - R2			R2	Daño físico	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac15 - R3			R3	Interrupción de servicio eléctrico	4	5	Riesgo extremo (20)	1	2	3	3	Riesgo medio (9)
Ac15 - R4			R4	Perdida del equipo	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac15 - R5			R5	Eliminación de información	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac15 - R6			R6	Error en configuración	2	5	Riesgo medio (10)	1	1	1	4	Riesgo bajo (4)
Ac21 - R1	Ac21	3CX Softphone	R1	Ingeniería social	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac21 - R2			R2	Interceptación de información	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac21 - R3			R3	Indisponibilidad de la aplicación	3	4	Riesgo medio (12)	2	2	1	2	Riesgo inusual (2)
Ac5 - R1	Ac5	Base de datos (SAPO)	R1	Fuga de información	2	3	Riesgo medio (6)	1	2	1	1	Riesgo inusual (1)
Ac5 - R2			R2	Acceso no autorizado	2	3	Riesgo medio (6)	1	2	1	1	Riesgo inusual (1)
Ac5 - R3			R3	Eliminación de información	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac5 - R4			R4	Modificación errada de la información	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)

Fuente: Autor

Cuadro 53 (continuación).

Código riesgo	Código activo	Activo	Riesgo	Amenaza	Probabilidad	Impacto	Nivel de riesgo Inherente	Reducción probabilidad	Reducción impacto	Nueva probabilidad	Nuevo impacto	Nivel de riesgo residual
Ac13 - R1	Ac13	Switches	R1	Acceso no autorizado	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac13 - R2			R2	Daño físico	2	5	Riesgo medio (10)					Riesgo bajo (3)
Ac13 - R3			R3	Interrupción de servicio eléctrico	4	5	Riesgo extremo (20)			3		Riesgo medio (9)
Ac13 - R4			R4	Perdida del equipo	2	5	Riesgo medio (10)			1		Riesgo bajo (3)
Ac13 - R5			R5	Manipulación errada de equipos	2	5	Riesgo medio (10)					Riesgo bajo (3)
Ac18 - R1	Ac18	Móviles Android	R1	Ingeniería social	2	4	Riesgo medio (8)	1	2	1	2	Riesgo inusual (2)
Ac18 - R2			R2	Perdida del dispositivo	3	4	Riesgo medio (12)			2		Riesgo bajo (4)
Ac18 - R3			R3	Acceso no autorizado	4	3	Riesgo medio (12)			3	1	Riesgo bajo (3)
Ac19 - R1	Ac19	Consola Antivirus	R1	Acceso no autorizado	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac19 - R2			R2	Indisponibilidad de la aplicación	2	5	Riesgo medio (10)					Riesgo bajo (3)
Ac19 - R3			R3	Error en configuración	2	5	Riesgo medio (10)					Riesgo bajo (3)

Fuente: Autor

Cuadro 53 (continuación).

Código riesgo	Código activo	Activo	Riesgo	Amenaza	Probabilidad	Impacto	Nivel de riesgo Inherente	Reducción probabilidad	Reducción impacto	Nueva probabilidad	Nuevo impacto	Nivel de riesgo residual
Ac2 - R1	Ac2	Computadores	R1	Acceso no autorizado	4	4	Riesgo alto (16)	1	2	3	2	Riesgo medio (7)
Ac2 - R2			R2	Interrupción de servicio eléctrico	4	5	Riesgo extremo (20)	1	2	3	3	Riesgo medio (9)
Ac2 - R3			R3	Perdida de equipo	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac2 - R4			R4	Daño físico	2	3	Riesgo medio (6)	1	2	1	1	Riesgo inusual (1)
Ac2 - R5			R5	Manipulación errada de equipos	2	5	Riesgo medio (10)	1	2	1	3	Riesgo bajo (3)
Ac23 - R1	Ac23	SW CRM (control operativo)	R1	Acceso no autorizado	3	4	Riesgo medio (12)	1	2	2	2	Riesgo bajo (4)
Ac23 - R3			R3	Denegación de servicio	2	3	Riesgo medio (6)	1	2	1	1	Riesgo inusual (1)
Ac10 - R1	Ac10	Go do Works Web	R1	Acceso no autorizado	2	3	Riesgo medio (6)	1	2	1	1	Riesgo inusual (1)
Ac10 - R3			R3	Fuga de información	2	3	Riesgo medio (6)	1	2	1	1	Riesgo inusual (1)
Ac10 - R4			R4	Denegación de servicio	2	3	Riesgo medio (6)	1	2	1	1	Riesgo inusual (1)
Ac11 - R1	Ac11	Go do Works Apk	R1	Acceso no autorizado	4	3	Riesgo medio (12)	1	2	3	1	Riesgo bajo (3)
Ac11 - R2			R2	Indisponibilidad de la aplicación	3	3	Riesgo medio (9)	1	2	2	1	Riesgo inusual (2)
Ac11 - R3			R3	Fuga de información	4	3	Riesgo medio (8)	1	2	3	1	Riesgo bajo (3)
Ac12 - R2	Ac12	SW Sapo	R2	Indisponibilidad de la aplicación	2	3	Riesgo medio (6)	1	2	1	1	Riesgo inusual (1)
Ac24 - R2	Ac24	SW Essential PIM	R2	Indisponibilidad de la aplicación	3	4	Riesgo medio (12)	2	2	1	2	Riesgo inusual (2)

Fuente: Autor

14. POLÍTICAS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

La construcción de la política de seguridad se realizó con base a los requerimientos que aplican para los procesos de Ofimarcas y se diseñaron en conjunto con el director de tecnología, siguiendo los lineamientos de la guía para la elaboración de la política general de seguridad y privacidad de la información publicada por Min tic la cual se definió dentro del marco teórico. Dentro de la guía se describe las políticas específicas recomendadas para la implementación de controles de seguridad de la información.

La postura de seguridad de la información dentro de Ofimarcas se representa en las políticas de seguridad de la información buscando proteger los activos de información como lo son software, hardware y toda información recopilada dentro de las actividades de la organización, dentro del marco de los tres pilares de la seguridad de la información, como lo son la disponibilidad, integridad y confidencialidad. Busca generar una cultura de seguridad dentro de sus colaboradores y aliados en cuantos al uso de los activos.

La política esta alineada con los dominios de la norma ISO 27001:2013, deberán ser ajustadas según el ciclo PHVA, buscando que se genere una mejora continua sobre los lineamientos y se realicen modificaciones periódicamente o cada que la organización así lo requiera.

Las políticas de Ofimarcas son de cumplimiento obligatorio y se deben asumir sin excepción por todos los colaboradores y proveedores de la compañía, en caso de incumplir cualquiera de las políticas la compañía procederá con la aplicación de sanciones. Toda sanción deberá estar acompañada por una investigación formal, que recopile la información necesaria como evidencia, dependiendo de la gravedad del incumplimiento, la investigación podrá ejecutarse de forma interna o externa, de tal forma que las sanciones internas serán definidas por Ofimarcas y las externas por entidades legales.

14.1 ALCANCE

Las políticas deben ser informadas y puestas en práctica por todos los colaboradores de la organización, en conjunto con los aliados que realicen actividades dentro de los procesos de Ofimarcas. Deben ser aplicadas buscando proteger todos los activos de información, de esta forma se apoya los objetivos estratégicos definidos por la compañía.

14.2 RESPONSABILIDADES

Los directores de Ofimarcas, son los responsables de liderar la gestión del sistema de seguridad de la información, deben garantizar la publicación, socialización y cumplimiento de las políticas por parte de todos los colaboradores y aliados que

participan en las actividades de la organización.

14.3 POLÍTICA GENERAL

Ofimarcas es consciente de la importancia de contar con procedimientos claros en cuanto al manejo de los activos de información, que permita a sus colaboradores actuar en cumplimiento de los tres pilares de la seguridad de la información, enfocando sus esfuerzos en apoyar los objetivos estratégicos de la compañía, así como dar cumplimiento a las leyes establecidas dentro de su objetivo de negocio.

14.3.1 Políticas organización de la seguridad de la información. La alta dirección de Ofimarcas está comprometida con el cumplimiento de las políticas de seguridad de la información por parte de todos los colaboradores de la organización, se debe realizar una definición de roles y responsabilidades acorde a las actividades que se desempeñan dentro de los procesos de Ofimarcas.

Compromiso de la alta dirección: Desde la alta dirección debe demostrar compromiso participando durante el diseño e implementación de del SGSI, adoptando las siguientes responsabilidades:

- Ofimarcas deberá mantener contacto con autoridades y grupos de intereses, que permita fortalecer los controles y seguridad de la información, así como con las autoridades para realizar escalamientos oportunos ante incidentes de seguridad.

- Los proyectos que definan y ejecuten dentro de Ofimarcas, deben contar con un recurso que tenga la capacidad de gestionar y garantizar el cumplimiento de la seguridad de la información durante su ejecución y entrega a la operación.

- Todos los recursos tecnológicos, dispositivos móviles y software asignados, son propiedad de la Ofimarcas, deben ser utilizados exclusivamente para las tareas asignadas dentro del rol en la compañía. Por esta razón la compañía se reserva el derecho de revisar y monitorear toda la información que se almacene dentro de estos dispositivos sin necesidad de realizar un previo aviso.

- Se debe hacer uso de bloqueo por código o patrones seguros de los dispositivos móviles asignados a los colaboradores.

- El colaborador no debe instalar aplicaciones en los dispositivos móviles entregados, esta actividad es realizada previamente por el área de tecnología.

- El colaborador solo tiene autorizado almacenar información en las herramientas aprobadas por la compañía, se prohíbe hacer uso de almacenamiento en equipos locales o repositorios no autorizados por Ofimarcas.

14.3.2 Seguridad de los recursos humanos. Se debe garantizar que los colaboradores y aliados comprendan las responsabilidades frente a la seguridad de la información.

Antes de asumir el empleo: El área de gestión humana debe contar con procedimientos aprobados que garanticen:

- Una contratación adecuada y alineada con las actividades que se va a ejecutar durante el rol de la convocatoria.

- Realizar las validaciones correspondientes para garantizar la veracidad de los documentos suministrados por el aspirante.

- Realizar directamente o por medio de un aliado, la validación de antecedes de acuerdo con las leyes establecidas.

- Los aspirantes deberán tener conocimiento de la política de seguridad de la información previo a la firma del contrato.

Durante la ejecución del empleo: Todos los colaboradores deben cumplir con los lineamientos de seguridad de la información establecidos, Ofimarcas debe mantener informados a los colaboradores en cuanto la ubicación y actualización de la política de seguridad.

Toma de conciencia, educación y formación en seguridad de la información: Todos los colaboradores deben cumplir con las capacitaciones relacionadas con la toma de conciencia de seguridad de la información, al inicio de su contrato como las definidas durante cada año.

Durante las capacitaciones de seguridad de la información se deben establecer mecanismos de medición donde el colaborador tome decisiones e interactúe con escenarios de la realidad.

Terminación y cambio de empleo: Cuando se genere un cambio de labores, ascenso o terminación del contrato, es deber de gestión humana:

- informar por medio de un documento que garantice el debido proceso y la no divulgación de información confidencial.

- Reportar por medio de correo electrónico la novedad al área de tecnología para que se ejecuten los respectivos procesos de gestión de accesos.

14.3.3 Gestión de activos. Responsabilidad por los activos: es responsabilidad del departamento técnico o tecnología, mantener actualizado y custodiado el formato inventario de activos de Ofimarcas, en este debe registrarse la siguiente

información:

- Identificador.
- Nombre del activo.
- Descripción de la función o información que procesa el activo.
- Tipo de activo.
- Ubicación del activo.
- Estado actual del activo, si este en encuentra en funcionamiento o no.
- Proceso que interviene con el activo de información.

Política de uso aceptable de los activos: Todos los equipos y sistemas de información son propiedad de Ofimarcas. El acceso y uso de estos activos, es exclusivo de personal que tenga una relación contractual con Ofimarcas y deberán ser destinados únicamente para las actividades asignadas dentro de la compañía.

Los propietarios de activos de información son responsables de cumplir con todas las políticas para dar un uso adecuado a los activos asignados en Ofimarcas.

Política clasificación de la información: Es responsabilidad de todos los colaboradores, realizar una debida clasificación de la información y el uso que se da a la misma dentro de los procesos en los que intervienen así:

- Información confidencial: Aquella que debe ser conocida únicamente por el funcionario para dar cumplimiento a sus actividades dentro del rol que cumple en Ofimarcas.

- Información de uso interno: Toda información que deben conocer los funcionarios de Ofimarcas y es trasmitida entre funcionarios o procesos para dar cumplimiento exclusivamente a sus actividades.

- Información pública: Es la información que puede ser conocida por cualquier persona tanto interna como externa a Ofimarcas.

Política de manejo de medios: Es responsabilidad del área de tecnología revisar los logs de los activos de información para garantizar que sean utilizados en actividades exclusivamente laborales, en caso de identificar anomalías, se debe reportar de inmediato al jefe inmediato del colaborador responsable de las tracciones identificadas.

Todos los colaboradores deben tener presente las siguientes directrices:

- Toda información contenida dentro de los equipos de la compañía son propiedad de Ofimarcas.

- Está prohibida la instalación de software que no esté aprobado por el área de

tecnología.

- Los equipos de cómputo no podrán ser reubicados o trasladados sin previa autorización del área de tecnología.

- Ningún colaborador podrá realizar configuraciones técnicas en los equipos de cómputo, es una actividad exclusiva del área de soporte en sitio.

- Se prohíbe el uso de medios extraíbles en cualquiera de los equipos asignados por la compañía. Este medio de conexión se deshabilitará en todos los equipos durante su fase de alistamiento.

- Se prohíbe la conexión de equipos de cómputo personales en la red corporativa de Ofimarcas.

- Los colaboradores son responsables de la información que sea descargada dentro de los equipos asignados por la compañía.

- El colaborador deberá bloquear la sesión de su equipo mientras no esté haciendo uso de este.

- Está prohibido utilizar correos personales en los equipos asignados para las actividades del rol en Ofimarcas.

14.3.4 Control de acceso. Requisitos del negocio para el control de acceso: Ofimarcas asignará los usuarios dependiendo del rol que el colaborador desempeña, la solicitud deberá enviarse al departamento técnico a través de un correo electrónico, por parte del jefe directo con previa autorización de gestión humana.

Política de control de acceso: Ofimarcas se compromete, a regular el acceso a los activos, sistemas de información e instalaciones, de acuerdo con la necesidad de cumplimiento de actividades exclusivas en la compañía.

Política de acceso a redes y a servicios en red: Solo los activos de información propiedad de Ofimarcas pueden acceder a la red corporativa.

Política de registro y cancelación del registro de usuarios: Solo los colaboradores autorizados podrán contar con acceso a la información necesaria para el cumplimiento de las actividades relacionadas con su rol, cuando los accesos no se requieran estos deberán ser eliminados.

Política de gestión de acceso de usuarios: El dueño de los activos es el responsable de asignar los permisos correspondientes de acuerdo el rol que desempeña el funcionario, el dueño del activo debe hacer entrega del acceso por medio de una

carta de responsabilidad la cual deberá ser firmada por parte del colaborador.

Política de gestión de derechos de acceso privilegiado: El nivel de privilegios de los usuarios en los sistemas de información debe ser asignado con base a los requeridos únicamente para dar cumplimiento a las actividades del rol que desempeña. Los derechos de acceso privilegiado deben ser revisados periódicamente.

Política responsabilidades de los usuarios: Está prohibido compartir usuarios y contraseñas de acceso a los sistemas de información, es deber del jefe inmediato garantizar que sus subordinados rindan cuentas de la información que manipulan dentro de las actividades de la organización.

Política de autenticación secreta: Las contraseñas deben cumplir con un nivel de complejidad de un mínimo de 9 caracteres, utilizando en su construcción mayúsculas, minúsculas, números y caracteres especiales. Las contraseñas deben ser cambiadas periódicamente y en caso de identificarse una vulneración a la seguridad.

Política de control de acceso a sistemas y aplicaciones: la asignación de roles debe realizarse con base a la matriz de accesos definida, controlando que información puntualmente requiere accederse dependiendo de la actividad que ejecuta el colaborador. Ofimarcas debe contar con un sistema para la gestión de contraseñas seguras, que permita al colaborador autogestionarlas.

Política de conexión segura: El acceso a los sistemas de información de Ofimarcas debe surtir un proceso de autenticación segura.

Política de gestión de contraseñas: Los sistemas de información deben implementar procesos que obliguen el cambio de contraseña cada 30 días o cuando así lo considere necesario el departamento de tecnología.

El cambio de contraseña deberá realizarse únicamente por el colaborador propietario y responsable de la cuenta, de ser necesario se realizará validación de datos personales.

14.3.5 Criptografía. Ofimarcas deberá utilizar un sistema que le permita cifrar la información que se considere confidencial, de tal forma que se garantice la confidencialidad al momento de almacenar o trasferir información, en cuanto a las características solo se podrá utilizar algoritmos que a la fecha no se hayan identificado vulnerabilidades y es deber del departamento de tecnología confirmar su robustez.

Política de uso de controles criptográficos: Se debe considerar los controles criptográficos para proteger la integridad y confidencialidad de los datos. De igual

forma se deben implementar procesos para administrar la generación, distribución, intercambio y revocación / destrucción de claves criptográficas.

14.3.6 Seguridad física y del entorno. Ofimarcas se compromete a controlar el acceso físico a las instalaciones que comprometen el almacenamiento de los activos de información de la compañía.

Política de perímetro de seguridad física: El acceso a las oficinas, cuartos de cómputo y todos los espacios donde se encuentren ubicados sistemas de información de Ofimarcas son considerados de acceso restringido.

Política de controles físicos de entrada: El acceso a las instalaciones de Ofimarcas debe ser gestionado por medio de controles de seguridad física, que permitan la identificación y acceso únicamente a los colaboradores autorizados.

Política de ubicación y protección de los equipos: Los activos físicos valorados como críticos, deben estar almacenados o ubicados en zonas de acceso restringido, solo los colaboradores según su rol tendrán acceso.

Política de servicios públicos de soporte: Los activos de información deben contar con controles que aseguren su protección antes fallas en servicios de soporte.

Política de seguridad del cableado: Todo el cableado que se utilice para la entrega de servicios a Ofimarcas debe estar certificado con estándares recomendados que cumplan con la disponibilidad, confidencialidad e integridad de la información.
Política mantenimiento de equipos: Se deben realizar mantenimientos periódicos a los equipos de Ofimarcas, buscando mantenerlos disponibles para su correcta operación y funcionamiento.

Política de escritorio y pantalla limpios: se debe concientizar a los colaboradores sobre un correcto manejo de la información, buscando proteger la confidencialidad, integridad y disponibilidad de la información física y digital.

14.3.7 Seguridad de las operaciones. Procedimientos operacionales y responsabilidades: Todos los procedimientos operativos deben estar documentados en un portal de procesos que sea de conocimiento y fácil acceso para todos los colaboradores, todo cambio que se genere debe quedar documentado y controlado mediante la gestión de cambios. Los lideres de los procesos son responsables de hacer seguimiento de los recursos necesarios para la ejecución de las actividades que garanticen el desempeño requerido de los activos y sistemas de información.

Política de protección contra códigos maliciosos o copias de respaldo: Se debe implementar sistemas de detección de intrusos que permita la detección, prevención y recuperación contra códigos maliciosos.

Política de separación de los ambientes de desarrollo, pruebas, y operacionales: Deben existir diferentes ambientes según la fase en la que se encuentre un protector o desarrollo, la información sensible que se utilice en ambientes de pruebas debe protegida con controles de enmarcamiento u ofuscamiento.

Todo cambio en sistemas operativos o aplicaciones deben ser realizados en ambiente de pruebas y cumplir satisfactoriamente con los requerimientos, previo a su despliegue en ambientes productivos.

Política de registro y seguimiento: es responsabilidad de los lideres de procesos monitorear el comportamiento de los accesos a los sistemas de información, así como todas las configuraciones que se realicen en los activos por parte de los administradores. Todos los registros deben ser almacenados y conservar de tal forma que se garantice la confidencialidad e integridad de estos, todos los sistemas de información deben sincronizarse con un único servidor ntp.

Política control de software operacional: Es responsabilidad del área de tecnología, identificar oportunamente las vulnerabilidades técnicas de los sistemas de información que utiliza Ofimarcas y tomar las medidas necesarias que minimicen su exposición. Solo está permitida la instalación de software autorizado por el área de tecnología y está será realizada únicamente por el personal técnico. El área de tecnología es responsable de planificar la revisión anual o cuando se requiera, de los sistemas operativos utilizados en la organización.

Política de copias de respaldo: Se deben implementar mecanismos y procedimiento que permitan almacenar y recuperar la información.

Se deben implementar copias de respaldo de todos los activos que almacenen y procesen información crítica de Ofimarcas, los medios y procedimientos de almacenamiento deben cumplir con estándares que garantice la protección de la confidencialidad, integridad y disponibilidad de la información.

Las copias de respaldo deben se probadas y validadas regularmente, de tal forma que se asegure su efectividad ante situaciones que requieran de su uso. Deben almacenarse en un sitio o ubicación diferente al que se encuentran los activos de producción, de tal forma que se proteja ante situaciones que afecten las instalaciones de Ofimarcas.

Política de registro de eventos: todas las transacciones y eventos que intervienen dentro de los procesos deben estar almacenados en un log que permita realizar la identificación del responsable de su ejecución. Todo sistema entregado a operación debe validarse que cumpla con este registro de eventos y se debe asegurar que no puedan ser desactivados o modificados.

Política de protección de la información de registro: El acceso a la información de

registro es restringido. El área de tecnología es quien está autorizada para brindar los accesos según se considere el caso y su finalidad.

Política de registros del administrador y operador: Todas las tracciones realizadas por los administradores de los sistemas de información se deben almacenar y proteger. Deben ser revisados periódicamente por el director de tecnología.

Política de sincronización de relojes: Todos los servidores deben estar sincronizados por medio de un servicio NTP que garantice un adecuado registro y seguimiento de la información.

Política de gestión de las vulnerabilidades técnicas: se debe validar constantemente los sistemas de información en busca de vulnerabilidades técnicas que puedan ser explotadas.

El área de tecnología es la única responsable y autorizada para ejecutar actividades de análisis de vulnerabilidades en los sistemas de información como en la red corporativa. El análisis debe incluir aplicaciones, redes, servidores, bases de datos y demás activos de información de los procesos críticos de Ofimarcas.

Del resultado de los análisis de vulnerabilidades, el área de tecnología es responsable de entregar un informe al comité directivo, que permita facilitar la toma de decisiones en cuanto los controles o soluciones que se deban implementar.

Los colaboradores no tienen permitido ejecutar software dentro de los sistemas de información de Ofimarcas sin una previa aprobación del área de tecnología.

14.3.8 Seguridad de las comunicaciones. Se debe garantizar la protección de la información que viaja a través de las redes y sistemas de información de Ofimarcas.

Política de controles de redes: El área de tecnología, es el único autorizado y responsable de acceder a los cuartos técnicos, así como de realizar las modificaciones y ajustes que consideren necesarios. En caso de requerir acceso de terceros, estos deben ser aprobados y supervisados por personal de tecnología.

Todos los elementos de red que componen la infraestructura de Ofimarcas, deben tener habitado el registro de logs y deben ser revisados periódicamente por el área de tecnología a fin de identificar transacciones anormales.

Política gestión de seguridad de redes: Se debe implementar las configuraciones en la red necesarias para garantizar la separación de las redes de los usuarios y los sistemas de información, esta arquitectura debe estar documentada y aprobada.

Política de transferencia de información: El único medio de transferencia aprobado por Ofimarcas es el correo corporativo asignado al colaborador y compartir información a través del one drive, está prohibido utilizar cualquier otro medio de

comunicación. En caso de ser necesaria la transferencia de información confidencial con terceros, se debe firmar acuerdos de confidencialidad y no divulgación, se debe realizar a través de protocolo sftp y con el cifrado por medio de llaves pgp.

Política de acuerdos de confidencialidad o de no divulgación: La información procesada debe ser trasferida única y exclusivamente dentro de las necesidades de Ofimarcas. Todos los colaboradores y contratistas deben conocer, aceptar y firmar los acuerdos de confidencialidad.

Los acuerdos de confidencialidad deben ser revisados regularmente y modificarse de ser necesario buscando proteger los intereses de Ofimarcas y cumplimiento legal que respecte.

14.3.9 Adquisición, desarrollo y mantenimiento de sistemas. Todo sistema que sea adquirido por Ofimarcas deberá contar implementar medidas de seguridad durante todo su ciclo de vida.

Política de análisis y especificación de requisitos de seguridad de la información: Todos los sistemas adquiridos por Ofimarcas, deben cumplir con los requisitos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información. Deben ser sometidos a análisis de vulnerabilidades y en caso de ser sistemas expuestos a internet, deben surtir un proceso de hacking ético.

La información que se utilice para realizar pruebas en los nuevos sistemas debe ser cruzada entre sí para garantizar que no exista información real durante las pruebas.

Es responsabilidad del área solicitante del nuevo sistema, realizar la recepción y seguimiento al sistema, así como de cumplir con todos los procedimientos de entrega a operación.

Política de seguridad de servicios de las aplicaciones en redes públicas: se debe proteger la información que es enviada desde la red interna hacia medios externos.

Los canales de comunicación con proveedor o entidades externas deben estar asegurados con protocolos seguros, la información transmitida debe estar cifrada durante su transferencia.

Política de protección de transacciones de los servicios de las aplicaciones: Todas las transacciones ejecutadas en Ofimarcas, deben estar protegidas de tal forma que se evite una transmisión incompleta, alteración de mensajes o divulgación no autorizada.

14.3.10 Relaciones con los proveedores. Todos los proveedores de Ofimarcas deben firmar los acuerdos de confidencialidad, así como acogerse a las políticas de seguridad de la información implementadas en la compañía, se debe dejar claridad

en los contratos de la información que será procesada por el proveedor, las responsabilidades de cara al cumplimiento de la seguridad de la información y las sanciones que se impondrán por el incumplimiento de las obligaciones contractuales.

Política de seguridad de la información en las relaciones con los proveedores: Se debe documentar y acordar los requisitos de cumplimiento de seguridad de la información que permita mitigar los riesgos asociados con el acceso de los proveedores a la información de Ofimarcas.

Los proveedores deben cumplir con estándares de seguridad adecuados y estos deben ser validados durante la fase de evaluación de proveedores. El área responsable de la contratación de los servicios del proveedor deberá realizar seguimiento a las actividades ejecutadas y reportar cualquier anomalía que se identifique.

Política de tratamiento de la seguridad dentro de los acuerdos con proveedores: Se deben establecer acuerdos de confidencialidad que protejan los activos de información de Ofimarcas, de tal forma que los proveedores que accedan a estos tengan conocimiento de los deberes y sanciones a las que se someten en caso de no dar cumplimiento de las políticas de seguridad de la información. El área gestora de la solicitud del proveedor debe solicitar apoyo del área legal con el fin establecer contractualmente todos los requisitos de cumplimiento.

Todos los proveedores y contratistas deben aceptar y firmar los lineamientos que se definan en Ofimarcas.

Política de cadena de suministro de tecnología de la información y comunicación: Todo equipo o sistema de información que sea de proveedores y sea utilizado por Ofimarcas, debe ser revisado y aprobado por el área de tecnología de tal forma que se garantice que cumplen con los requisitos de seguridad.

Política de seguimiento y revisión de los servicios de los proveedores: Se debe hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores que contrata Ofimarcas buscando garantizar la continuidad de la operación.

Política de gestión de cambios a los servicios de los proveedores: Los cambios sobre los servicios de los proveedores, deben ser informados y evaluados por el comité directivo, es responsabilidad del área ejecutora del contrato, realizar seguimiento de los servicios. Todo cambio debe estar documentado y debidamente registrado en los logs de los sistemas que se intervengan.

14.3.11 Gestión de incidentes de seguridad de la información. Se debe garantizar una adecuada gestión de los incidentes de seguridad que se presenten

en Ofimarcas.

Política de responsabilidades y procedimientos: Todos los colaboradores deben informar al área de tecnología cualquier evento que consideren anormal que esté relacionado con la seguridad de la información.

Es deber del área de tecnología identificar, priorizar y dar respuesta a los incidentes de seguridad que se reporten, tomando las acciones que den a lugar, para garantizar la confidencialidad, integridad y disponibilidad de la información, adicional deberá generar un informe detallando el incidente y reportarlo al comité directivo. Desde el área de tecnología se debe informar al comité directivo los recursos necesarios para contar con una adecuada gestión de seguridad en los activos de información de Ofimarcas.

El comité directivo es respónsale de revisar el informe y en conjunto tomar las medidas que se consideren necesarias para dar tratamiento al incidente.

14.3.12 Aspectos de seguridad de la información de la gestión de continuidad de negocio. Se debe determinar los requisitos de seguridad de la información y la continuidad de las operaciones ante situaciones adversas.

Política de redundancias: Se deben implementar controles que permitan contar con una adecuada redundancia de los servicios eléctricos y de comunicaciones. Se debe establecer un plan de continuidad de negocio que estructure dentro del documento, áreas de escalamiento, tiempos de respuesta, operación en contingencia y un responsable de la activación del plan.

Los planes de continuidad deben ser probados y monitoreados, en caso de ser necesario deberán ajustarse conforme se presenten modificaciones en los procesos, tareas o activos de información involucrados en el proceso.

14.3.13 Cumplimiento. Es responsabilidad de los directivos garantizar y dar cumplimiento de las normativas establecidas para la seguridad de la información, evitando incumplir obligaciones legales o contractuales, es una actividad que debe ser acompañada por el área legal.

Política de identificación de la legislación aplicable y de los requisitos contractuales: El área legal es el responsable de identificar y documentar todos los requisitos estatutarios, reglamentarios y contractuales que apliquen para Ofimarcas y sus sistemas de información.

Política de derechos de propiedad intelectual: todos los colaboradores de Ofimarcas deben proteger y respetar la propiedad intelectual de la compañía, así como la propiedad intelectual de otros.

Todo software o sistema que se adquiera debe ser a través de proveedores autorizados o directamente con el fabricante, de tal modo que se respete el licenciamiento y derechos de autor.

Es prohibido copiar y distribuir el software adquirido por Ofimarcas, para fines distintos a los establecidos por la compañía, el área de tecnología es el único autorizado para instalar, remover o modificar versiones del software y es responsable de resguardar y custodiar el software y licencias adquiridas por Ofimarcas.

Política de protección de registros: El área legal en conjunto con el dueño del activo o información es el responsable de implementar controles que protejan los registros, contra perdida, destrucción, falsificación y acceso no autorizado de acuerdo con los requisitos legislativos de reglamentación, contractuales y del negocio.

Política de privacidad y protección de información de datos personales: El área de gestión humana es el responsable de proteger y almacenar los datos personales que se transmitan en Ofimarcas dando cumplimiento a la ley 1581 de 2012.

Política de revisión independiente de la seguridad de la información: El comité directivo es responsable de revisar, el enfoque de Ofimarcas para la gestión de seguridad de la información y su implementación en intervalos planificados o cuando ocurran cambios significativos.

Cumplimiento con las políticas y normas de seguridad: Los dueños de los activos deben revisar que se cumplan con los requisitos de seguridad de la información y reportar al área de tecnología al momento de identificar anomalías.

Política de revisión del cumplimiento técnico: Es responsabilidad del área de tecnología, revisar periódicamente los sistemas, para determinar el cumplimiento y normas de seguridad de la información.

15. PLAN DE SENSIBILIZACIÓN

15.1 INTRODUCCIÓN

Para la construcción del plan de sensibilización se tomó como guía el plan de capacitación, sensibilización y comunicación de seguridad de la información publicado por Min tic, el cual se definió dentro del marco teórico del documento.

Mediante este documento se define el plan de capacitación y sensibilización de todos los aspectos relacionados con la seguridad de la información en la compañía Ofimarcas para los colaboradores, internos y/o externos.

15.2 OBJETIVO

Lograr que todos los colaboradores y aliados de Ofimarcas, conozcan y comprendan el sistema de gestión de seguridad de la información que está definido dentro de la compañía, así como sus políticas y procedimientos enfocados en disminuir la posibilidad de que se materialicen incidentes de seguridad que afecten alguno de los pilares de la seguridad como los son, la disponibilidad, integridad y confidencialidad.

15.3 ALCANCE

Está enfocado a todos los colaboradores internos y externos que tenga vinculación con la organización, empleados, proveedores y aliados que por el desarrollo de sus actividades tengan acción directa o indirecta sobre los activos de información de Ofimarcas.

15.4 ROLES Y RESPONSABILIDADES

15.4.1 Gerencia. La gerencia de Ofimarcas debe garantizar los recursos necesarios para que todos los colaboradores tengan la posibilidad de acceder al plan de capacitación y sensibilización, la gerencia debe permanecer en constate seguimiento de la ejecución de las actividades y evaluar las mismas para identificar su eficacia, en caso de identificar mejoras se deben realizar acciones correctivas que permitan cumplir las expectativas de Ofimarcas.

15.4.2 Líderes de los procesos. Un líder de proceso por la naturaleza de su cargo es quien más conoce la forma en como los colaboradores interactúan con la información de la compañía, por este motivo se requiere una participación activa en el proceso de capacitación y sensibilización, deben realizar propuestas que se alineen con los objetivos de seguridad de la información y buscar desde el ejemplo la correcta aplicación de las políticas y procedimientos que se definieron dentro de Ofimarcas para garantizar los tres pilares de la seguridad de la información.

15.4.3 Proveedores y/o Terceros. Al tener una relación directa con las actividades de Ofimarcas, deben estar contextualizados con cada una de las actividades del plan de capacitación y sensibilización, comprometerse con la incorporación de los protocolos definidos para la ejecución de las actividades, se deben realizar retroalimentación y seguimiento para garantizar que se cumpla con las buenas prácticas de seguridad definidas en la compañía.

15.4.4 Colaboradores. Todos los colaboradores deben estar comprometidos con las actividades del plan de capacitación y sensibilización definido dentro de Ofimarcas y a dar cumplimiento en la ejecución de las actividades diarias tomando como base los conocimientos adquiridos durante la formación.

15.4.5 Grupo de comunicaciones. En Ofimarcas se debe delegar un grupo de comunicaciones que este conformado por personal del área de tecnología y de gestión humana que en conjunto elaboren los textos que se van a enviar o publicar, esta información debe estar aprobada por el director de tecnología previo a su divulgación, se sugiere que Ofimarcas contrate una compañía que ofrezca servicios de diseño para la elaboración de contenidos. Es responsabilidad del grupo de comunicaciones garantizar el cumplimiento de actividades que se plantean en el documento y cronograma.

15.5 METAS

La compañía Ofimarcas mediante la ejecución del plan de capacitación y sensibilización busca alcanzar las siguientes metas:

- Socializar con todos sus colaboradores y aliados la existencia del sistema de gestión de seguridad de la información definido en la compañía, así como todos su protocolos y procedimientos.

- Dar a conocer y reforzar las definiciones, protocolos y políticas establecidas para fortalecer la seguridad de la información en cada una de las actividades que se ejecutan.

- Evaluar los conocimientos y aplicabilidad de las buenas prácticas y protocolos por parte de todos los involucrados en los procesos de la compañía.

15.6 POBLACIÓN DESTINO

El plan de sensibilización tiene como población destino:

- Empleados de Ofimarcas.
- Aliados y terceros de Ofimarcas.

15.7 RECURSOS

Para el desarrollo del plan, Ofimarcas puede disponer de su personal para ejecutar las actividades de acuerdo con su rol dentro de la organización, así como las plataformas que actualmente tienen desplegadas para la comunicación con sus empleados mediante el uso de las herramientas de office 365. Para la comunicación con aliados y terceros se debe realizar a través del correo electrónico.

15.8 DIVULGACIÓN

Por la disposición actual de las actividades en Ofimarcas, es necesario utilizar métodos de divulgación digitales y flexibles para que la sensibilización se torne dinámica, estos pueden variar según la necesidad, la población destino o el tema que se va a socializar, los métodos que se podrían aplicar son:

15.8.1 funcionarios internos

- Publicaciones en la intranet de la compañía.
- Talleres de sensibilización con el uso de presentaciones.
- Fondos de pantalla.
- Capacitaciones a través de medios digitales.
- Folletos digitales.
- Herramientas de Office 365.

15.8.2 Aliados y terceros:

- Infografías, folletos y boletines informativos a través del correo electrónico.

- Los recursos necesarios para el cumplimiento de las actividades deben garantizarse por parte de la alta gerencia de Ofimarcas, actualmente la compañía se puede apoyar en herramientas como Office 365.

15.9 DESCRIPCIÓN TEMAS SUGERIDOS DE SENSIBILIZACIÓN Y CAPACITACIÓN

15.9.1 Contexto del SGSI. Se debe contextualizar los temas del sistema de gestión de seguridad de la información, logrando que se entienda de forma clara las necesidades y ventajas de su aplicación, así como la participación de cada uno de los colaboradores dentro del cumplimiento de los objetivos del SGSI en Ofimarcas.

15.9.2 Políticas del SGSI. Consiste en dar a conocer las políticas de seguridad de la información a todos los colaboradores, logrando un entendimiento claro de la política general y las políticas de cada uno de los dominios del SGSI, para lograr una mayor comprensión se debe utilizar ejemplos con las tareas del día a día de

Ofimarcas, se debe contar con evidencia en cuanto que los colaboradores comprenden las políticas y conocen su ubicación de tal forma que la puedan consultar cuando lo consideren.

15.9.3 Incidentes de seguridad de la información. Brindar una explicación de los eventos u ocurrencias que atentan contra la confidencialidad integridad y disponibilidad de la información, se puede utilizar ejemplos visuales que describan una situación de afecte cada uno de los pilares de la seguridad de la información, es importante que los colaboradores conozcan cada concepto:

- Confidencialidad: Solo acceden a la información las personas que previamente fueron autorizadas

- Integridad: La información no puede ser modificada sin una previa autorización

- Disponibilidad: Se debe garantizar el acceso a la información en todo momento.

15.9.4 Aplicaciones seguras. Mostrar la importancia de instalar y utilizar únicamente el software que este aprobado por el área de tecnología, debido a que cualquier otro aplicativo de fuentes desconocidas, podría generar una brecha de seguridad.

15.9.5 Escritorio limpio. Generar conciencia a los colaboradores de la importancia de no tener documentos confidenciales a simple vista o de fácil acceso, es importante que los colaboradores clasifiquen la información que utilizan de tal forma que la información que ya no requieren utilizar para sus actividades sea archivada de forma segura. Conservar la pantalla del equipo de cómputo libre de archivos, los cuales podrían ser copiados, utilizados o estar al alcance de terceros o por personal que no cuente con permisos para su acceso.

15.9.6 Backups. Sensibilizar a los funcionarios de Ofimarcas respecto a la importancia de realizar backups de la información que se considera critica para la ejecución de las actividades según el rol, ejemplarizar escenarios de perdida de información como puede ser por un ataque de ramsonware mostrando como solución el contar con la información respaldada.

15.9.7 Fuga de información. Dar a conocer los escenarios que pueden deliberar en una salida o exposición de información que ocasiona que esta llegue a personas no autorizadas o sobre la que su responsable pierde el control, es un escenario que se puede presentar por un inadecuado uso de herramientas tecnológicas y que puede comprometer la confidencialidad de la información de la compañía.

15.9.8 Fraude online. Buenas prácticas que ayuden a reducir la probabilidad de ser víctimas de fraude online:

- Comprobar la ortografía y redacción de la página.
- Verificar el origen del acceso a la página ¿Por qué se encuentra en ella?
- ¿Responde a una solicitud previamente realizada?
- ¿Existe algún tipo de relación o servicio con la página que está visitando?

15.9.9 Clasificación de la información. Es el proceso que consiste en que el propietario o custodio de la información evalúa, los datos que posee y el nivel de protección o confidencialidad que cada uno requiere. El objetivo es que se comparta únicamente la información necesaria y al personal indicado, para dar cumplimiento exclusivamente a las actividades del rol que desempeña en Ofimarcas, el funcionario debe comprender los siguientes aspectos:

- Información confidencial: Aquella que debe ser conocida únicamente por el funcionario para dar cumplimiento a sus actividades dentro del rol que cumple en Ofimarcas y que, dado el nivel de importancia dentro de sus funciones, requiere conservarse con máxima privacidad.

- Información de uso interno: Toda información que deben conocer los funcionarios de Ofimarcas y es trasmitida entre funcionarios o procesos para dar cumplimiento exclusivamente a sus actividades.

- Información pública: Es la información que puede ser conocida por cualquier persona tanto interna como externa a Ofimarcas.

15.9.10 Seguridad en smartphone. Al existir la asignación de este tipo de dispositivos móviles en Ofimarcas, es importante que sus funcionarios conozcan que a través de este se procesa información de Ofimarcas y que deben seguirse recomendaciones de seguridad:

- Se debe establecer autenticación para acceder al dispositivo, se puede utilizar, contraseñas, pin o patrones de seguridad.

- Solo el funcionario debe acceder a su dispositivo asignado.

- El smartphone debe destinarse exclusivamente para actividades de Ofimarcas y con las aplicaciones autorizadas por el área de tecnología.

- Reportar al área de tecnología cualquier novedad que se presente con el dispositivo asignado.

15.9.11 Correo electrónico seguro. Dar a conocer buenas prácticas que permitan a los usuarios utilizar el correo corporativo de tal manera que no se comprometa la seguridad de la compañía:

- Identificar el remitente del correo.

- Ser cautelosos al momento de abrir enlaces.
- No responder correos spam.
- Precaución al momento de descargar archivos adjuntos.
- Correo electrónico exclusivo para actividades de Ofimarcas.

15.9.12 Contraseñas seguras. Se debe orientar a los colaboradores de tal forma que, al momento de generar sus contraseñas de acceso, lo hagan con criterios que permitan contar con una contraseña robusta como se establece en la política de seguridad de la información, se debe dar a conocer ejemplos de cuanto podría tardar un atacante en identificar una contraseña dependiendo de las características de esta.

15.9.13 Bloqueo de sesión. Mostrar la importancia de asegurar la información contenida dentro del equipo, bloqueando la sesión mientras se está ausente del puesto de trabajo, en este escenario se puede plantear ejemplos donde se ejecuten transacciones en el equipo de la víctima sin la previa autorización o sin el consentimiento de esta.

15.9.14 Navegación segura. Recomendaciones que permiten al usuario navegar de forma segura en la web por medio de los equipos asignados en Ofimarcas.

- Visitar sitios con protocolo seguro (https).
- No almacenar credenciales en el navegador.
- Precaución al navegar mediante conexión inalámbrica públicas.
- Evitar la descargar archivos de páginas no seguras.

15.9.15 Malware. Los funcionarios deben conocer la definición de malware. Es un programa que en su lógica está diseñado para realizar actividades que afectan los pilares de la seguridad de la información, este tipo de programas puede ser distribuido a través de correo electrónico, páginas web, chats, entre otros y se busca engañar a la víctima para que permita su ejecución.

15.9.16 Phishing. Es una técnica que se utiliza para engañar a las víctimas, se debe dar a conocer el concepto de phishing, como evitar ser víctima y mostrar ejemplos claros de cómo se ejecutan.

15.9.17 Protección de datos personales. Dar conocimiento a los colaboradores sobre la existencia de leyes que obligan a las compañías a la aplicación de medidas y controles que permitan la protección de datos personales. La ley 1581, tiene el objeto de desarrollar el derecho constitucional que tienen todas las personas para conocer, actualizar y rectificar la información que haya sido recolectada de ellos en bases de datos o archivos.

15.10 FRECUENCIA DE ACTIVIDADES

El cuadro 54 muestra la frecuencia de las actividades.

Cuadro 54. Frecuencia temas sugeridos

Temas	Objetivo	Actividad o método	Frecuencia
Contexto del SGSI.	Divulgar el SGSI entre las partes interesadas y que se conozca su importancia dentro de los objetivos de la compañía.	Enviar un comunicado a través del correo electrónico, enumerando la importancia del SGSI en Ofimarcas.	Una vez al año.
Política de seguridad.	Lograr que los colaboradores identifiquen y acepten las políticas de seguridad de la información dentro de sus actividades diarias, así como su ubicación.	Publicar en la intranet un comunicado donde se informe de la existencia y ubicación del documento, incentivando al colaborador a consultarlo.	Una vez al año.
Incidentes de seguridad y aplicaciones seguras.	Comprender cuando se presenta un incidente de seguridad y generar conciencia sobre el software que se utiliza en los equipos.	Charla con el personal de tecnología, utilizando ejemplos que permitan al colaborador reportar incidentes de seguridad, durante la sesión mostrar las desventajas de utilizar aplicaciones de fuentes desconocidas o que no hacen parte de las aprobadas por el área de tecnología.	Una vez al año.
Escritorio Limpio.	Generar conciencia sobre las ventajas que se obtienen al mantener organizado el escritorio y la información del equipo.	Video donde se muestre un funcionario sin seguir las buenas prácticas y otro donde si se apliquen, al finalizar se deben destacar la importancia de hacerlo.	Una vez al año.
Backups.	Identificar la importancia de realizar backups de la información como control y como buena práctica.	Enviar un comunicado a través del correo electrónico que muestre las ventas de realizar backups de la información.	Una vez al año.
Fuga de información y fraude online.	Evitar que los funcionarios realicen actividades que favorezcan la materialización de la fuga de información e identifiquen como pueden evitar ser víctimas de páginas fraudulentas.	Realizar un taller virtual, donde a través de una presentación, se dé a conocer las diferentes formas en que se puede fugar la información y que tipo de fraude online se puede ser víctima.	Una vez al año.
Clasificación de la información.	Fortalecer los conceptos de clasificación de información y su importancia.	Charla con el personal de tecnología, utilizando ejemplos donde el colaborador clasifique la información.	Una vez al año.
Seguridad en smartphone.	Lograr que los colaboradores utilicen el smartphone con buenas prácticas de seguridad.	Video donde se explique cómo realizar la configuración adecuada de pin y contraseñas en el smartphone y al final listar las buenas prácticas.	Una vez al año.

Cuadro 54 (Continuación)

Temas	Objetivo	Actividad o método	Frecuencia
Correo electrónico seguro y contraseñas seguras.	Asegurar que los colaboradores dan buen uso del correo electrónico y la construcción de contraseñas robustas.	Enviar un mail con una imagen, donde se ilustre las recomendaciones para el uso del correo y ejemplos de contraseñas seguras.	Una vez al año.
Bloqueo de sesión y navegación segura.	Disminuir la posibilidad de que los colaboradores dejen su equipo desatendido y mejorar las habilidades de la navegación web.	Entregar volantes informativos a los colaboradores, donde se explique las bondades de bloquear la sesión y seguir las recomendaciones para navegar de forma segura.	Una vez al año.
Malware y phishing.	Fortalecer conceptos en cuanto a los ataques que puede afectar una compañía.	A través de posters físicos en las oficinas, mostrar los conceptos de Malware y phishing.	Una vez al año.
Protección de datos personales.	Contextualizar a los colaboradores en cuanto a la importancia de dar cumplimiento a las leyes.	Charla con el personal de tecnología en conjunto con el área legal, donde se contextualice la ley 1581.	Una vez al año.

Fuente: Autor

15.11 CRONOGRAMA DE ACTIVIDADES

En Ofimarcas se diseñó un cronograma, como se aprecia en el cuadro 55, el cual debe ser ejecutado por el grupo de comunicaciones, este documento se establece a un año y define los temas que se deben ejecutar en cada uno de los meses, así como la población objetivo. Los medios de comunicación que actualmente tiene Ofimarcas es a través de Office 365, de esta forma pueden enviar los comunicados a través de Teams y correo electrónico para el personal interno, para proveedores y terceros se debe utilizar el correo electrónico. El material físico que consideren compartir con sus funcionarios debe ser diseñado e impreso por una compañía que brinde este tipo de servicios.

Cuadro 55. Cronograma

Comunicaciones seguridad de la información.																								
Temas	**Enero**		**Febrero**		**Marzo**		**Abril**		**Mayo**		**Junio**		**Julio**		**Agosto**		**Septiembre**		**Octubre**		**Noviembre**		**Diciembre**	
Contexto del SGSI.																								
Política de seguridad.																								
Incidentes de seguridad y aplicaciones seguras																								
Escritorio Limpio.																								
Backups.																								
Fuga de información y fraude online																								
Clasificación de la información.																								
Seguridad en smartphone.																								
Correo electrónico seguro y contraseñas seguras																								
Bloqueo de sesión y navegación segura																								
Malware y phishing																								
Protección de datos personales																								
								Personal interno									Aliados y terceros							

Fuente: Autor

15.11.1 Evaluación y resultados. Deben existir métodos de evaluación para cada una de las actividades, es importante identificar si las actividades son exitosas y en caso de que se requiera se debe hacer los ajustes necesarios que permitan mejorar el nivel de conciencia y aplicación de la seguridad de la información dentro de Ofimarcas. Existen plataformas que permiten evaluar los conceptos que se dispongan dentro del plan de formación una de ellas es Google forms, a través de esta plataforma se puede realizar formularios tipo cuestionario y por medio de un enlace al cual acceden los funcionarios, se puede evaluar los conceptos y así contar con un seguimiento en cuanto la efectividad del plan.

15.12 MATERIALES DE EJEMPLO

De la figura 11 a la 18 se evidencian algunos ejemplos relacionados con recomendaciones sobre temas de seguridad informática.

Figura 14. Ejemplo 1.

Fuente: OSI - Oficina de seguridad del internauta. [en línea]. Bogotá: La entidad [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.osi.es/es>

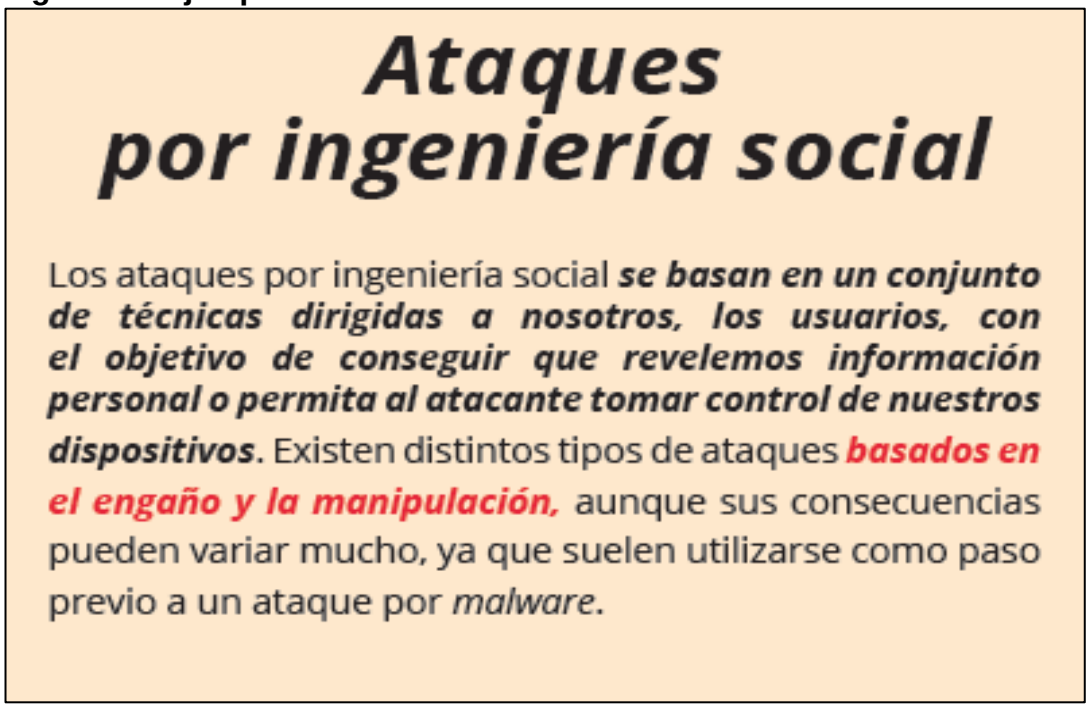
Figura 15. Ejemplo 2.

Fuente: OSI - Oficina de seguridad del internauta. [en línea]. Bogotá: La entidad [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.osi.es/es>

Figura 16. Ejemplo 3.

Fuente: OSI - Oficina de seguridad del internauta. [en línea]. Bogotá: La entidad [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.osi.es/es>

Figura 17. Ejemplo 4.



Fuente: OSI - Oficina de seguridad del internauta. [en línea]. Bogotá: La entidad [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.osi.es/es>

Figura 18. Ejemplo 5.

Fuente: OSI - Oficina de seguridad del internauta. [en línea]. Bogotá: La entidad [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.osi.es/es>

Figura 19. Ejemplo 6.

Fuente: OSI - Oficina de seguridad del internauta. [en línea]. Bogotá: La entidad [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.osi.es/es>

Figura 20. Ejemplo 7.

Fuente: OSI - Oficina de seguridad del internauta. [en línea]. Bogotá: La entidad [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.osi.es/es>

Figura 21. Ejemplo 8.

Fuente: OSI - Oficina de seguridad del internauta. [en línea]. Bogotá: La entidad [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.osi.es/es>

16. CONCLUSIONES

- Con el diseño del sistema de gestión de seguridad de la información, se logró establecer una serie de controles, políticas de seguridad de la información y un plan de concientización, los cuales le permiten a Ofimarcas contar con herramientas para administrar la seguridad de sus activos de información.

- La gestión de la seguridad de la información requiere de una estrategia que se adapte a las necesidades del negocio y requiere apoyo de la alta gerencia en la asignación de recursos para el cumplimiento de las actividades y de esta forma demuestran su compromiso.

- Al identificar el estado actual de los procesos críticos de Ofimarcas respecto a los dominios y controles de la norma ISO/IEC 27001:2013, se concluyó que su nivel de cumplimiento es bajo y no se está protegiendo los activos de información adecuadamente.

- Con la identificación, clasificación y valorización de activos de información se logró definir cuáles son los activos más importantes dentro de la operación de los procesos críticos de Ofimarcas y fue el punto de partida para el análisis de riesgos.

- A través de la metodología de riesgos que se definió en Ofimarcas, se logró identificar los riesgos a los que están expuestos los activos de información y con base a los criterios de aceptación reconocer los riesgos que debían ser tratados.

- Con base a los controles del anexo A de la norma ISO/IEC 27001:2013, se estableció el tratamiento para los riesgos no aceptables por Ofimarcas, obteniendo el riesgo residual para cada uno de ellos.

- La construcción de políticas de seguridad de la información alineadas con los dominios y controles de la norma ISO/IEC 27001:2013 y el plan de sensibilización, permitió a Ofimarcas documentar herramientas que apalancan la estrategia del SGSI.

17. RECOMENDACIONES

Las recomendaciones que a continuación se sugieren son con base a mi experiencia como ingeniero de seguridad informática y a la información recopilada durante la ejecución de las actividades y los aspectos que se considera deben ser reforzados dentro de Ofimarcas.

Se debe documentar y publicar los procesos y procedimientos de los procesos de preventa, venta, postventa y soporte de Ofimarcas, estos deben estar aprobados por la alta gerencia. En el mercado existen diferentes plataformas que permiten realizar la gestión de procesos, una de ellas es ADONIS, un software como servicio (Saas), que permite documentar, estandarizar y mejorar los procesos de las compañías, facilitando la disponibilidad de la información para que esta sea accedida por el personal de la organización.

Se debe documentar, validar, revisar y aprobar por la alta gerencia la política de seguridad de la información, estableciendo una periodicidad mínima de un año o cuando Ofimarcas así lo considere. Adicionalmente debe ser socializada a todos los colaboradores y proveedores de Ofimarcas, deben existir mecanismos de aceptación, un ejemplo de ello es utilizar un formulario web posterior a la socialización de las políticas y a través de este recopilar el conocimiento por parte de los colaboradores.

Se debe realizar seguimiento del catálogo de activos de información por parte del líder de tecnología, una sugerencia es contar con el catálogo en formato Excel, el cual puede estar publicado en un SharePoint, que esté disponible para los empleados, pero su acceso a modificación este restringido a los lideres o directores de cada área.

Se debe valorar y clasificar la información o los activos de información de acuerdo con su nivel de criticidad teniendo en cuenta:

- información confidencial.
- información de uso por la empresa.
- información de dominio público.

La actividad de clasificación regularmente debe ser realizada por el propietario del activo, dado que es quien conoce que tan importante es su información y los impactos que podrían causar tras la materialización de una amenaza. Contar con este tipo de clasificación permite reducir a la probabilidad de compartir información confidencial, debe quedar claro dentro de los funcionarios que hay información que otras personas no requieren conocer para ejecutar sus actividades. Office 365 cuenta con un módulo que permite agregar etiquetas de confidencialidad a los archivos compartidos por correo, la funcionalidad impide que los archivos sean descargados, modificados o reenviados en contextos donde no es necesario, de

esta forma se reduce la fuga de información. Estas configuraciones deben ser administradas desde la consola de Office365 y crear manuales que permitan a los colaboradores utilizar este etiquetado cuando así lo requieran.

Se debe documentar planes de contingencia para los procesos críticos de Ofimarcas (preventa, venta, postventa y soporte), este plan debe ser probado bajo un esquema de contingencia, el plan consiste en identificar los impactos potenciales que amenacen las actividades de Ofimarcas, esto permitirá contar con un marco de referencia que permite contar con una resiliencia y la capacidad de actuar eficazmente, protegiendo así los intereses de la organización. Durante la construcción del plan se deben identificar aspectos primordiales como: tiempo objetivo de recuperación (RTO), punto objetivo de recuperación (RPO) y Periodo Máximo admisible de interrupción (MTPD), en la actualidad existe la norma ISO 22301, la cual especifica los requisitos para ayudar a las organizaciones a prevenir, preparar, responder y recuperarse de incidentes inesperados.

Se debe contar con una línea base de seguridad para las fábricas que desarrollan software para Ofimarcas. Inicialmente dentro de las políticas de seguridad de la información, se debe establecer un lineamiento que obliguen a todos los proveedores a cumplir con los lineamientos de desarrollo seguro, estos lineamientos se pueden definir dentro de un manual, que haga parte de los documentos que se firman entre las dos partes, dentro de este manual se establece los diferentes criterios de desarrollo para los productos tecnológicos que contrate Ofimarcas, por ejemplo: Manejo de sesiones, controles de autenticación, almacenamiento de información, protección de código fuente, uso web services, recolección de datos personales entre otros que considere la organización. Adicionalmente solicitar a las fábricas las buenas prácticas de desarrollo seguro que tengan definidas dentro su organización.

Se sugiere que todos los desarrollos cuenten con un análisis de vulnerabilidades previo a la puesta en producción, en caso de identificar vulnerabilidades el responsable del proyecto debe entregar un plan de tratamiento que reduzca la probabilidad de que las vulnerabilidades sean explotadas, actualmente existen herramientas que permiten realizar este tipo de análisis, por ejemplo, Qualiz, sin embargo, es recomendable contratar un servicio especializado para este tipo de actividades.

Dependiendo del tipo de desarrollo, exposición de la información o criticidad del proyecto para Ofimarcas, se debe considerar realizar un análisis de hacking ético, esta inspección es realizada por un humano, el cual simula un ataque real y tiene como objetivo penetrar la seguridad de la infraestructura tecnología realizando la explotación de vulnerabilidades en busca de comprometer sistemas críticos o información confidencial, de esta forma se puede contar con una visual actual del nivel de seguridad informática de Ofimarcas en su infraestructura tecnológica.

BIBLIOGRAFÍA

ALCALDÍA MAYOR DE BOGOTÁ. informe de auditoría TIC Bogotá. [en línea]. Bogotá: La entidad [citado 9 de octubre, 2021]. Disponible en Internet: < URL: http://www.desarrolloeconomico.gov.co/transparencia/control/reportes-control-interno/informe-auditoria-proceso-gestion-tics-2021>.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 100. (23, diciembre de 1993). Por la cual se crea el sistema de seguridad social integral y se dictan otras disposiciones. Bogotá, 1990. 51 p.

_ ___ _ _ _ _, _ _ _ _ _ _ _ _ _ Ley 378. (9, julio de 1997). Por medio de la cual se aprueba el "Convenio número 161, sobre los servicios de salud en el trabajo" adoptado por la 71 Reunión de la Conferencia General de la Organización Internacional del Trabajo, OIT, Ginebra, 1985. Bogotá, 1997. 29 p.

_ ___ _ _ _ _, _ _ _ _ _ _ _ _ _ Ley 46. (2, diciembre de 1988). Por la cual se crea y organiza el Sistema Nacional para la Prevención y Atención de Desastres, se otorga facultades extraordinarias al presidente de la República, y se dictan otras disposiciones. Bogotá, 1988. 63 p.

_ ___ _ _ _ _, _ _ _ _ _ _ _ _ _ Ley 50. (28, diciembre de 1990). Por la cual se introducen reformas al Código Sustantivo del Trabajo y se dictan otras disposiciones. Bogotá, 1990. 51 p.

_ ___ _ _ _ _, _ _ _ _ _ _ _ _ _ Ley 717. (24, diciembre de 2001). Por la cual se establecen términos para el reconocimiento de las pensiones de sobrevivientes y se dictan otras disposiciones. Bogotá, 2001. 29 p.

_ ___ _ _ _ _, _ _ _ _ _ _ _ _ _ Ley 769. (6, julio de 2002). Por la cual se expide el Código Nacional de Tránsito Terrestre y e dictan otras disposiciones. Bogotá, 2002. 29 p.

_ ___ _ _ _ _, _ _ _ _ _ _ _ _ _ Ley 776. (17, diciembre de 2002). Por la cual se dictan normas sobre la organización, administración y prestaciones del Sistema General de Riesgos Profesionales. Bogotá, 2002. 29 p.

_ ___ _ _ _ _, _ _ _ _ _ _ _ _ _. Ley 82. (23, diciembre de 1982). Por medio de la cual se aprueba el Convenio 159 sobre la readaptación profesional y el empleo de personas inválidas, adoptado por la Conferencia General de la Organización Internacional del Trabajo en su 69a. reunión, Ginebra, 1983. Bogotá, 1982. 39 p.

_ ___ _ _ _ _, _ _ _ _ _ _ _ _ _ Ley 9. (24, enero de 1979). Por medio de la cual se dictan medidas sanitarias. Bogotá, 1979. 39 p.

DIARIO PORTAFOLIO. Aumentan en 30% los ataques cibernéticos en Colombia. [en línea]. Bogotá: La Empresa [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.portafolio.co/tendencias/aumentan-en-30-los-ataques-ciberneticos-en-colombia-553803>.

ENTERPRISE IT. SGSI. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://enterpriseit.cl/>
https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>

ICONTEC. Instituto de Normas Técnicas y Certificación. Norma Técnica Colombiana. NTC-ISO-IEC 27001:2013. Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. Bogotá: Icontec. p.4

ISO. International Organization for Standardization. ISO 31000:2018. Gestión del riesgo — Directrices. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es.

ISO. International Organization for Standardization. ISO/CEI 27001:2013. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>.

ISO. International Organization for Standardization. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Requisitos. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.iso.org/standard/54534.html>

ISO27001.es. Términos y Definiciones. [en línea]. Bogotá: La entidad [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.iso27000.es/sgsi.html>

ISOTools. ¿En qué consiste el ciclo PHVA de mejora continua? [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/>

MinTIC. Ministerio de Tecnologías de la Información y Comunicaciones. Guía No. 2. Elaboración de la política general de seguridad y privacidad de la información. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL:

MinTIC. Ministerio de Tecnologías de la Información y Comunicaciones. Guía 14. Plan de Comunicación, Sensibilización, Capacitación. [en línea]. Bogotá: La entidad

[citado 12 de abril, 2022]. Disponible en Internet: < URL: https://gobiernodigital.mintic.gov.co/portal/Categor-as/Seguridad-y-Privacidad-de-la-Informacion/150525:Plan-de-capacitacion-sensibilizacion-y-comunicacion-de-seguridad-de-la-informacion>.

NORMAS ISO 27001. Referencias normativas. [en línea]. Bogotá: La entidad [citado 12 de abril, 2022]. Disponible en Internet: < URL: https://normaiso27001.es/referencias-normativas-iso-27000/#terminos.

OFIMARCAS. Información institucional interna. Bogotá, 2022.p.11.

OFIMARCAS. Información Institucional. [en línea]. Bogotá: La entidad [citado 9 de octubre, 2021]. Disponible en Internet: < URL: https://www.ofimarcas.com/>.

OSI - Oficina de seguridad del internauta. [en línea]. Bogotá: La entidad [citado 3 de junio de 2022]. Disponible en Internet: < URL: https://www.osi.es/es>.

ANEXOS

ANEXO A. PRESUPUESTO

		Mensual			Proyecto	
	ITEM	Unidades	Valor unidad	Total, Mensual	Meses	Total
1	Servicio Energía	1	$ 60,000	$ 60,000	2	$ 120,000
2	Servicio Internet	1	$ 70,000	$ 70,000		$ 140,000
3	Desplazamientos	1	$ 100,000	$ 100,000		$ 200,000
4	Alimentación	1	$ 20,000	$ 20,000		$ 40,000
5	Papelería	1	$ 20,000	$ 20,000		$ 40,000
6	Honorarios	1	$ 3,500,000	$ 3,500,000		$ 7,000,000
7	Aplicaciones y elementos de comp	1	$ 250,000	$ 250,000		$ 500,000
8	Servicio de telefonía	1	$ 30,000	$ 30,000		$ 60,000
	Sub total mensual		$ 4,050,000	$ 4,050,000		
	Total, proyecto					**$ 8,100,000**

ANEXO B. CRONOGRAMA

		Marzo			Abril				Mayo				Junio				Julio			
	Actividad / Semana	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Contexto de la organización																			
2	Alcance del SGSI																			
3	Diagnóstico inicial																			
4	Análisis de los 11 dominios de la Iso27001:2013																			
5	Informe estado de los dominios																			
6	Identificación de activos																			
7	Gestión de riesgos																			
8	Valoración de controles																			
9	Diseño de políticas de seguridad de la información																			
10	Diseño del plan de sensibilización																			