CONSEJO PROFESIONAL
DE MEDICINA VETERINARIA Y DE ZOOTECNIA DE COLOMBIA

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD DE LA INFORMACIÓN
PROCESO TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
VERSIÓN 15-12-2023

TABLA DE CONTENIDO

Contenido

1. GENERALIDADES Y CONTEXTO 9
1.1. SUPERVISIÓN, CONTROL Y AUDITORÍA 10
1.2. EXCEPCIONES 10
1.3. INCUMPLIMIENTO DE LAS POLÍTICAS DESCRITAS EN ESTE DOCUMENTO 11
2. TERMINOLOGÍA Y DEFINICIONES 11
3. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN 12
3.2. OBJETIVOS ESPECÍFICOS 12
4. COMPROMISO CON EL CUMPLIMIENTO DE LOS REQUISITOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 13
5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 13
DECLARACIÓN GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 13
5.1 OBJETIVOS DE LA POLÍTICA DE SGSI: 13
SEGURIDAD DE LOS RECURSOS INFORMÁTICOS 14
5.2. GUIA DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 14
5.2.1. Directrices para la Seguridad de la Información 14
5.2.2. Revisión de las Políticas para la Seguridad de la Información 15
6.ORGANIZACIÓN DE LA SEGURIDAD 15
6.1. ESTRUCTURA INTERNA 15
6.1.1. Funciones y Obligaciones para la Seguridad de la Información 15
6.1.2 Separación de Funciones 16
6.1.3 Contacto con Autoridades 16
6.1.4 Contacto con grupos de Interés especial 17
6.1.5 Seguridad de la Información en la Gestión de Proyectos 17
6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO 17
6.2.1 Política para Dispositivos Móviles. 17
6.2.2 Teletrabajo 18

7. SEGURIDAD DE LOS RECURSOS HUMANOS 20
7.1 ANTES DE ASUMIR EL EMPLEO 20
7.1.1 Selección 20
7.1.2 Términos y condiciones del empleo 20
7.2 DURANTE LA EJECUCIÓN DEL EMPLEO 20
7.2.1 Responsabilidades de la Dirección 20
7.2.2Toma de Conciencia, educación y Formación en seguridad de la información. 21
7.2.3 Proceso disciplinario 21
7.3 TERMINACIÓN Y CAMBIO DE EMPLEO 22
7.3.1Terminación o cambio de responsabilidades de empleo 22
8. GESTIÓN DE ACTIVOS. 22
8.1 RESPONSABILIDAD POR LOS ACTIVOS 22
8.1.1 Inventario de activos. 22
Adquisición y asignación de equipos de usuario 22
Activos críticos 23
8.1.2 Propiedad de los activos 23
8.1.3 Uso aceptable de los activos 23
Uso general 23
Uso de computadores 24
Uso de Internet 25
Uso de correo electrónico y mensajería instantánea 26
Servicios de red 28
Uso de las aplicaciones corporativas 28
Uso de la red inalámbrica 28
8.1.4 Devolución de activos 29
8.2 CLASIFICACIÓN DE LA INFORMACIÓN 29
8.2.1 Clasificación de la información 29
8.2.2 Etiquetado de la información 31
8.2.3 Manejo de Activos 32

8.3 MANEJO DE MEDIOS 32
8.3.1 Gestión de medio removibles 32
8.3.2 Disposición de los medios 33
8.3.3 Transferencia de Medios 33
9. CONTROL DE ACCESO 34
9.1 REQUISITO DEL NEGOCIO PARA CONTROL DE ACCESO 34
9.1.1 Política de control de acceso 34
9.1.2 Acceso a redes y servicios de red 34
9.2 GESTIÓN DEL ACCESO A USUARIOS 36
9.2.1 Registro y cancelación del registro de usuarios 36
9.2.2 Suministro de acceso de usuarios 36
9.2.3 Gestión de derechos de acceso privilegiado 37
9.2.4 Gestión de Información de Autenticación Secreta de Usuarios 37
9.2.5 Revisión de los derechos de acceso de los usuarios. 39
9.2.6 Retiro o Ajuste de los derechos de acceso 39
9.3 RESPONSABILIDADES DE LOS USUARIOS 40
9.3.1 Uso de información de autenticación secreta 40
9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES 40
9.4.1 Restricción de acceso a la información 40
9.4.2 Procedimiento de Ingreso seguro 40
9.4.3 Sistema de gestión de contraseñas 41
9.4.4 Uso de programas utilitarios privilegiados 41
9.4.5 Control de acceso a código fuente de programas 41
10. CRIPTOGRAFÍA 41
10.1 CONTROLES CRIPTOGRÁFICOS 41
10.1.1Política sobre el uso de controles criptográfico 41
10.1.2 Gestión de llaves 43
11.1 ÁREAS SEGURAS 44
11.1.1 Perímetro de seguridad física 44

11.1.2 Controles de acceso físico 45
11.1.3 Seguridad de oficinas, recintos e instalaciones 46
11.1.4 Protección contra amenazas externas y ambientales 47
11.1.5 Trabajo en áreas seguras 47
11.1.6 Áreas Públicas Áreas de Despacho y Carga 47
11.2 SEGURIDAD DE LOS EQUIPOS 48
11.2.1 Ubicación y protección de los equipos 48
11.2.2 Servicios de suministro 49
11.2.3 Seguridad del cableado 49
11.2.4 Mantenimiento de los equipos 49
11.2.5 Retiro de activos 50
11.2.6 Seguridad de equipos y activos fuera de las instalaciones 50
11.2.7 Disposición segura o reutilización de equipos 50
11.2.8 Equipos de usuario desatendido 51
11.2.9 Política de escritorio despejado y de pantalla despejada 51
12. SEGURIDAD DE LAS OPERACIONES 51
12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES 51
12.1.1 Procedimientos de operaciones documentados 51
12.1.2 Gestión de cambios 52
12.1.3 Gestión de capacidad 52
12.1.4 Separación de los entornos de desarrollo, pruebas y producción 53
12.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS 53
12.2.1 Controles contra códigos maliciosos 53
12.3. COPIAS DE RESPALDO 55
12.3.1 Respaldo de la información 55
12.4 REGISTRO Y SEGUIMIENTO 55
12.4.1 Registro de eventos 55
12.4.2 Protección de la información de registro 56
12.4.3 Registros del administrador y del operador 56

12.4.4 Sincronización de relojes 56
12.5 CONTROL DE SOFTWARE OPERACIONAL 57
12.5.1 Instalación de Software en Sistemas Operativos 57
12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA 57
12.6.1 Gestión de la vulnerabilidad técnica 57
12.6.2 Restricciones sobre la instalación de software 58
12.7. CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN 58
12.7.1 Controles sobre auditorias de sistemas de información 58
13. GESTIÓN DE LA SEGURIDAD DE LAS COMUNICACIONES. 59
13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES 59
13.1.1 Controles de las redes 59
13.1.2 Seguridad de los servicios de la red 60
13.1.3 Separación en las redes 60
13.2 TRANSFERENCIA DE INFORMACIÓN 61
13.2.1 Políticas y procedimientos para la transferencia de información 61
13.2.2 Acuerdos para la transferencia de información 62
13.2.3 Mensajería Electrónica 63
13.2.4 Acuerdo de confidencialidad o no divulgación 64
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 65
14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN 65
14.1.1 Análisis y especificaciones de requisitos de seguridad de la información 65
14.1.2 Seguridad de servicios de las aplicaciones en redes públicas 66
14.1.3 Protección de transacciones de los servicios de las aplicaciones 66
14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE 67
14.2.1 Política de desarrollo seguro 67
14.2.2 Procedimientos de control de cambios en sistemas 68
14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación 69
14.2.4 Restricciones en los cambios a los paquetes de software 69

14.2.5 Principios de construcción de sistemas seguros 70
14.2.6 Ambiente de desarrollo seguro 70
14.2.7 Desarrollo contratado externamente 71
14.2.8 Pruebas de seguridad de sistemas 72
14.2.9 Prueba de aceptación de sistemas 72
14.3 DATOS DE PRUEBA 72
14.3.1 Protección de datos de prueba 72
15. RELACIONES CON LOS PROVEEDORES 73
15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS 73
15.1.1 Seguridad de la información para las relaciones con proveedores 73
15.1.2 Tratamiento de la seguridad dentro de acuerdos con proveedores 73
15.1.3 cadena de suministro de tecnología de información y comunicación 73
15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES 74
15.2.1 Seguimiento y revisión de los servicios de los proveedores 74
15.2.2 Gestión de cambios en los servicios de los proveedores 74
16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 74
16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN 74
16.1.1 Responsabilidades y procedimientos 74
16.1.2 Reporte de eventos de seguridad de la información 74
16.1.3 Reporte de debilidades de seguridad de la información 75
16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos 75
16.1.5 Respuesta a incidentes de seguridad de la información 75
16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información 75
16.1.7 Recolección de evidencia 76
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 76
17.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN 76
17.1.1 Planificación de la continuidad de la seguridad de la información 76
17.1.2 Implementación de la continuidad de la seguridad de la información 76

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. 77
17.2 REDUNDANCIAS 77
17.2.1 Disponibilidad de instalaciones de procesamiento de información 77
18. CUMPLIMIENTO 78
18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES 78
18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales 78
18.1.2 Derechos de propiedad intelectual 78
18.1.3 Protección de registros 79
18.1.4 Protección de los datos y privacidad de la información relacionada con los datos personales. 79
18.1.5 Reglamento de controles criptográficos 79
18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN 79
18.2.1 Revisión independiente de la seguridad de la información 80
18.2.2 Cumplimiento con las políticas y normas de seguridad 80
18.2.3 Revisión de cumplimiento técnico 80
19. DUDAS Y RECOMENDACIONES 80

DECLARACIÓN DE POLÍTICA DE SEGURIDAD

El vertiginoso avance de la tecnología, la fluidez de la información, la interoperabilidad de los sistemas y la búsqueda constante de conocimiento son elementos cruciales en la competencia por la sostenibilidad empresarial en mercados globales y regionales. La información representa un poder de decisión invaluable, permitiendo estimaciones del pasado, presente y futuro para orientar a la organización hacia un camino sostenible. La tecnología ha posibilitado nuevas formas de mercado y servicios en el mundo globalizado, con notables innovaciones en sectores como transporte, salud, educación, entretenimiento e industria.

Todo esto se trata del acceso a datos e información que respalde decisiones acertadas para asegurar el éxito o la supervivencia. Dentro de las organizaciones, la tecnología se erige como la herramienta principal para el flujo y gestión de datos. Los departamentos de Tecnologías de la Información (TI) y el Sistema de Gestión de Seguridad de la Información (SGSI) aplican políticas y controles para gestionar la información corporativa, protegiéndola de accesos no autorizados, fugas de datos, malware, ataques informáticos y otras amenazas. Además, estos procesos permiten asegurar los sistemas de información corporativos y gestionar nuevas tecnologías en busca de eficiencia.

EL CONSEJO PROFESIONAL plasma en este manual sus políticas de seguridad de la información, basadas en la norma NTC-ISO 27001:2022, referente para construir un SGSI que, mediante buenas prácticas y normativas vigentes, gestione eficientemente los riesgos de seguridad de la información para los servicios ofrecidos.

No se trata de restringir a usuarios o colaboradores, sino de optimizar su labor garantizando acceso eficiente a sistemas e información necesarios para su desempeño. Este documento detalla directrices de seguridad para operar los sistemas informáticos de EL CONSEJO PROFESIONAL, normativas, estándares, procedimientos e instrucciones, límites para usuarios y colaboradores, y lineamientos para aplicar y configurar servicios de redes y equipos en diferentes oficinas, estableciendo parámetros para una gestión segura de servicios, activos e información.

Esta política de seguridad de la información también es aplicable a aliados o terceros con relaciones contractuales.

1. GENERALIDADES Y CONTEXTO

El presente compendio ofrece las pautas esenciales para asegurar y/o resguardar los activos de información, así como los datos e información corporativa pertenecientes o procesados por EL CONSEJO PROFESIONAL. Las políticas actuales se aplican a todos los empleados o colaboradores de EL CONSEJO PROFESIONAL, incluyendo personal temporal, terceros que brindan servicios (outsourcing) ya sea en modalidad in-house u out-house, afiliados, proveedores y cualquier persona natural o jurídica que participe en transacciones, contrataciones o prestación de servicios con EL CONSEJO PROFESIONAL. Para los empleados o colaboradores de EL CONSEJO PROFESIONAL, la responsabilidad de asegurar el cumplimiento de estas políticas no recae únicamente sobre ellos, sino también en cada Presidente, Coordinador o Director, quienes deben supervisar y gestionar la ejecución efectiva de las mismas.

La SEGURIDAD INFORMÁTICA, consiste en proteger el software, el hardware y los datos de amenazas o peligros tales como:

- Uso y/o copias ilegales de software
- Pérdida de información
- Virus informático
- Fallas técnicas
- Robo
- Vandalismo
- Acceso no autorizado, entre otros.

Para proteger estos recursos informáticos es necesario, no solo el uso de la tecnología, sino también la colaboración de todos los funcionarios.

Un mecanismo eficaz que contribuye a minimizar la ocurrencia de las amenazas o peligros en la seguridad de la información es la correcta aplicación que le den los funcionarios a las políticas, normas y medidas preventivas contempladas en este manual.

Todos los funcionarios del CONSEJO PROFESIONAL MVZ, son responsables por los recursos informáticos que manejan (hardware, software y datos), teniendo la obligación de cumplir con todos los lineamientos que se dan en las presentes políticas

1.1. SUPERVISIÓN, CONTROL Y AUDITORÍA

La supervisión del cumplimiento de las políticas por parte de funcionarios, proveedores o terceros recae en el conocimiento que tenga cada coordinador o responsable de la administración de un servicio sobre el desempeño y cumplimiento de las obligaciones adquiridas. Se deben realizar las gestiones correspondientes para hacer cumplir las políticas e informar sobre cualquier incumplimiento.

El Oficial de Seguridad de la Información o Profesional Administrador del SGSI será el encargado de gestionar (Supervisión, Control y Auditoría) el cumplimiento de las políticas y/o controles técnicos y organizativos, así como las auditorías internas o externas. Además, se encargará de asegurar el cumplimiento de las políticas por parte del personal del CONSEJO PROFESIONAL MVZ o cualquier otro involucrado, con el objetivo de mejorar la seguridad de la información. Las auditorías están detalladas en el Manual del SGSI, en el numeral 10.2 "Auditoría Interna".

1.2. EXCEPCIONES

En caso de requerir excepciones a alguna de las políticas descritas, se deben solicitar a través del coordinador del funcionario, con la aprobación del secretario(a), o coordinador de cada área. Las excepciones deben documentarse y almacenarse mediante el formato web de Solicitud de

Servicios de Tecnología (Procedimiento de Gestión de Requerimientos). El evaluador de excepciones, con apoyo del área de Tecnologías de la Información y Telecomunicaciones si es necesario, evaluará los riesgos asociados. Si se determina que una excepción presenta riesgos elevados para la seguridad de la información, puede no autorizarse o ser escalada a un nivel jerárquico superior según la estructura organizativa de EL CONSEJO PROFESIONAL.

Las excepciones a políticas y privilegios serán revisadas anualmente, con fecha de vencimiento al 31 de diciembre de cada año. Si una excepción está vencida, debe solicitarse nuevamente mediante el formato de Solicitud de Servicios de Tecnología y las autorizaciones respectivas.

1.3. INCUMPLIMIENTO DE LAS POLÍTICAS DESCRITAS EN ESTE DOCUMENTO

El acatamiento de las políticas de seguridad de la información es obligatorio para todo funcionario, colaborador, contratista, consultor, pasante o tercera parte involucrada. En caso de detectar un incumplimiento, desacato o potencial violación a las políticas, ya sea por negligencia o intencionalmente, el colaborador que identifica la falta tiene la obligación de informarla mediante correo electrónico al coordinador del funcionario, con copia al Coordinador de Seguridad y Protección de Datos a la dirección registro@consejoprofesionalmvz.gov.co. Este último informará a las áreas pertinentes según el incidente, con el fin de tomar las medidas correctivas correspondientes y seguir el proceso disciplinario según el código vigente. Si el incidente involucra a un tercero como proveedor o cliente, se analizará conjuntamente con las partes dentro del CONSEJO PROFESIONAL, quienes tomarán las acciones necesarias para resolver la situación.

Es importante señalar que la falta de conocimiento no exime de responsabilidad en el cumplimiento de la política.

2. TERMINOLOGÍA Y DEFINICIONES

Este documento emplea los términos y definiciones establecidos por las normas ISO 27001 y 27002. A continuación, se resaltan los términos más relevantes con sus respectivas definiciones:

Información: Conjunto de datos que proporcionan detalles sobre algún aspecto.
Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad: Propiedad de la información que impide su divulgación o acceso por parte de individuos, entidades o procesos no autorizados.

Integridad: Propiedad de la información relacionada con su exactitud y totalidad.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando es requerida por una entidad autorizada.

Amenaza: Causa potencial de un incidente no deseado, capaz de ocasionar daños a un sistema o a la organización.

Evento de Seguridad de la Información: Ocurrencia identificada del estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, una falla en las salvaguardas, o una situación previamente desconocida relevante para la seguridad.

Incidente de Seguridad de la Información: Un solo evento o una serie de eventos no deseados o inesperados relacionados con la seguridad de la información, que poseen una significativa probabilidad de comprometer las operaciones comerciales y amenazar la seguridad de la información.

3. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

3.1. OBJETIVO GENERAL

Administrar y ejecutar en el área de Tecnologías de la Información y Telecomunicaciones de manera adecuada, los elementos que componen la gestión de la Seguridad de la Información del Consejo Profesional, para garantizar la operatividad de los servicios tecnológicos de la organización, asegurando la confidencialidad, integridad y disponibilidad de la información.

3.2. OBJETIVOS ESPECÍFICOS

- Establecer una metodología sólida de Gestión del Riesgo de Seguridad de la Información en Tecnologías de la Información (TI), manteniendo niveles de riesgo aceptables y permitiendo acciones efectivas para la mitigación, eliminación, transferencia o aceptación de riesgos.
- Diseñar, implementar y mejorar políticas y controles de seguridad de la información que protejan los activos de información, asegurando la confidencialidad, integridad y disponibilidad, especialmente en el Data Center de EL CONSEJO PROFESIONAL.
- Desarrollar un plan de concientización en seguridad de la información que fortalezca la aplicación de buenas prácticas en el uso de tecnologías de la información y comunicación, con el objetivo de reducir la materialización de incidentes de seguridad de la información.
- Fomentar una "Cultura de Seguridad y Control Informático" en el CONSEJO PROFESIONAL MVZ, sensibilizando a los funcionarios sobre la importancia de proteger equipos, software y datos de la entidad.
- Salvaguardar la información contra cualquier acceso no autorizado, evitando el uso indebido, copia, publicación o modificación accidental o intencional del software adquirido o desarrollado por EL CONSEJO PROFESIONAL MVZ, para garantizar su confiabilidad, integridad y disponibilidad.
- Cumplir con normas, políticas, procedimientos y medidas preventivas de seguridad definidas para el manejo de equipos de cómputo e información sistematizada.
- Clarificar las responsabilidades individuales de cada funcionario en relación con el manejo de información y equipos de cómputo.

4. COMPROMISO CON EL CUMPLIMIENTO DE LOS REQUISITOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Es fundamental que todos los funcionarios y partes interesadas en el CONSEJO PROFESIONAL MVZ se comprometan plenamente con el acatamiento de las políticas y controles establecidos. La Presidencia y Secretaría deben asumir un compromiso esencial brindando respaldo fundamental para la implementación efectiva del Sistema de Gestión de Seguridad de la Información (SGSI) y promoviendo la cultura de seguridad en todas las unidades de la organización.

En cuanto a los compromisos necesarios para cumplir con los requisitos del SGSI, como parte integral del liderazgo, se proporciona información detallada sobre los roles, responsabilidades y autoridades de la organización. Estos detalles pueden ser consultados en el presente documento.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

DECLARACIÓN GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

La política general de seguridad de la información refleja el compromiso y la postura del CONSEJO PROFESIONAL MVZ en relación con la salvaguarda del proceso misional y la Protección de Datos Personales, fundamentales para el logro de los objetivos de la entidad. Este compromiso se respalda mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la entidad.

En este documento se definen las políticas de seguridad de la información en concordancia con la norma ISO 27001:2022, el Manual del SGSI y las necesidades específicas del CONSEJO PROFESIONAL. Estas políticas se estructuran en secciones, numerales y apartados para facilitar su comprensión, estudio, implementación y aplicabilidad.

5.1 OBJETIVOS DE LA POLÍTICA DE SGSI:

- Generar confianza en Directivos, Socios, funcionarios, Protegidos y Proveedores relacionados con la garantía de la información y datos personales.
- Asegurar el cumplimiento de políticas, manuales y procedimientos respaldados por el SGSI para la seguridad de los procesos misionales y protección de datos personales en la entidad.
- Facilitar el cumplimiento normativo requerido por entes de control asociados a la seguridad de la información y protección de datos personales.
- Brindar apoyo continuo para garantizar la continuidad del negocio mediante la seguridad de los procesos misionales.

SEGURIDAD DE LOS RECURSOS INFORMÁTICOS

EL CONSEJO PROFESIONAL MVZ tiene motivos fundamentales para resguardar tanto la información como los equipos informáticos, entre los cuales destacan:

VALOR DE LA INFORMACIÓN: La información representa un activo crucial para la organización. La pérdida de esta puede resultar en costos significativos para su recuperación, tanto en términos económicos como operativos.

SERVICIO: Es imperativo proteger la información y los equipos informáticos para garantizar la continuidad de las operaciones y servicios ofrecidos tanto a usuarios internos como externos del CONSEJO PROFESIONAL MVZ.

LEGALIDAD: La presencia de copias ilegales de software en los equipos informáticos infringe la Ley 23 de 1982, el Decreto 1360 de junio 23 de 1989 y la Ley 44 de 1993 sobre Derechos de Autor, exponiendo a EL CONSEJO PROFESIONAL MVZ a multas y demandas onerosas que pueden afectar su imagen institucional. Se incluye la Ley 1581 de 2012 para garantizar el derecho fundamental de Hábeas Data y la protección de datos de los protegidos, clientes, contratistas y proveedores.

PROTECCIÓN DE LA INFORMACIÓN: Dada la naturaleza confidencial y estratégica de la información en manos del CONSEJO PROFESIONAL MVZ, se busca evitar su uso indebido por parte de terceros con fines fraudulentos y competencia desleal, en cumplimiento del Decreto 1377 de 2013, que reglamenta la Ley 1581 de 2012.

PRODUCTIVIDAD: La pérdida de tiempo al recuperar información sin copias de respaldo, ya sea por borrado accidental, ataques de virus informático o acceso no autorizado, puede impactar negativamente la productividad.

INTERACCIÓN FUNCIONARIOS - COMPUTADOR: El computador es una herramienta fundamental en la gestión administrativa de los funcionarios del CONSEJO PROFESIONAL MVZ.

PROTECCIÓN DE LA INVERSIÓN: Un uso adecuado y cuidadoso de los recursos informáticos contribuye a prolongar la vida útil de los sistemas computacionales.

5.2. GUIA DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

5.2.1. Directrices para la Seguridad de la Información

Todos aquellos con responsabilidades sobre fuentes, repositorios y recursos de procesamiento de información en EL CONSEJO PROFESIONAL, incluyendo funcionarios, personal externo y proveedores, deben adherirse a los principios establecidos en este documento y en documentos relacionados, los cuales han sido aprobados por la Presidencia y la secretaria ejecutiva. Estos principios abarcan políticas adaptadas a los sistemas tecnológicos de información y la estructura organizativa actual, asegurando niveles adecuados de confidencialidad, integridad y disponibilidad de la información.

Estas políticas de seguridad de la información se alinean con las estrategias, el entorno, los contratos y las legislaciones aplicables a EL CONSEJO PROFESIONAL. Se establecen para abordar temas como control de acceso, clasificación de información, seguridad física y del entorno, directrices para usuarios finales (uso aceptable de activos, transferencia de información, dispositivos móviles y teletrabajo, restricciones, entre otros), copias de respaldo o backups, protección contra código malicioso, gestión de vulnerabilidades, seguridad en las telecomunicaciones, privacidad y protección de información personal, y relaciones con proveedores, entre otros aspectos relacionados con la seguridad de la información.

Este documento y sus políticas de seguridad de la información han sido aprobados por la Junta Directiva, la Presidencia y la Coordinación de Tecnologías de la Información y Telecomunicaciones mediante el Acuerdo N°2327 - Declaración y Aprobación del Sistema de Gestión de la Seguridad y Políticas de Seguridad de la Información para EL CONSEJO PROFESIONAL.

5.2.2. Revisión de las Políticas para la Seguridad de la Información

Con el objetivo de garantizar una mejora continua en las políticas de la entidad, la Coordinación de Seguridad de la Información, con el respaldo de otros procesos, llevará a cabo, al menos una vez al año, una revisión de la política de seguridad de la información de EL CONSEJO PROFESIONAL MVZ, o cuando se produzcan cambios significativos en los procesos o sistemas, con el fin de identificar mejoras o la necesidad de ajustes. Una vez aprobados los cambios o ajustes a la Política, se llevará a cabo la respectiva divulgación o comunicación.

El Coordinador de Seguridad de la Información y Protección de Datos, así como el Profesional Administrador de SGSI, tendrán la autoridad para actualizar las Políticas de Seguridad de la Información según las necesidades de revisión y con la aprobación de la Coordinación de Tecnologías de la Información y Telecomunicaciones, la secretaría general y la Presidencia. La revisión se realizará al menos una vez al año, o antes, en caso de cambios significativos dentro de la organización, garantizando así que las políticas sean apropiadas, eficaces y eficientes para la empresa.

Las áreas correspondientes podrán desarrollar, revisar y evaluar las políticas de seguridad de la información relacionadas con ellas, trabajando en conjunto con el Administrador de Seguridad de la Información y siguiendo los protocolos de aprobación de nuevas políticas o cambios en las existentes. Se fomenta la comunicación de retroalimentaciones, sugerencias o inquietudes al correo registro@consejoprofesionalmvz.gov.co.

6.ORGANIZACIÓN DE LA SEGURIDAD

6.1. ESTRUCTURA INTERNA

6.1.1. Funciones y Obligaciones para la Seguridad de la Información

A continuación, se detallan las funciones y responsabilidades pertinentes en este documento.

Presidente / Secretaria Ejecutiva: Activa promoción de una cultura de seguridad de la información tanto interna como externamente. Garantiza los recursos, infraestructura y talento humano necesarios para implementar y mantener el SGSI.

Coordinación de Seguridad de la Información: EL CONSEJO PROFESIONAL cuenta con un responsable de seguridad de la información o Profesional Administrador SGSI, encargado de gestionar y mantener el Sistema de Gestión de Seguridad de la Información, en el cual se regulan las políticas de seguridad de la información.

Oficial o Técnico de Tecnología: Encargado de salvaguardar los datos personales de colaboradores, afiliados, usuarios, proveedores, etc., vinculados con EL CONSEJO PROFESIONAL en relación a las funciones definidas en el Manual de Funciones. Se ha designado al Coordinador de Seguridad de la Información como responsable del SGSI y del seguimiento del oficial.

Colaboradores: Funcionarios y personal proporcionado por terceros que desempeñan labores en o para EL CONSEJO PROFESIONAL tienen la responsabilidad de adherirse estrictamente a las políticas, normas, procedimientos y estándares relacionados con la seguridad de la información. Son responsables de los activos asignados, incluidos los de información, y deben informar eventos o incidentes de seguridad que puedan afectar a EL CONSEJO PROFESIONAL. Además, deben mantener la confidencialidad, integridad y disponibilidad de la información bajo su custodia.

Terceros y/o Aliados: Las terceras partes interesadas o aliadas de EL CONSEJO PROFESIONAL deben cumplir con las políticas de seguridad de la información establecidas en este documento. Deben utilizar la información de manera responsable dentro de un marco de seguridad que garantice la Confidencialidad, Integridad y Disponibilidad de la información o datos intercambiados, en el contexto de contratos o alianzas estratégicas.

6.1.2 Separación de Funciones

EL CONSEJO PROFESIONAL MVZ se encuentra estructurada por macroprocesos, procesos y subprocesos de tal manera que se pueda orquestar una operatividad acorde con los objetivos organizacionales. Para la seguridad de la información se implementa el SGSI dentro del área de Tecnologías de la Información y Telecomunicaciones, donde se definen roles para la administración del Data Center. Las funciones del equipo que administra los, aplicativos, redes y telecomunicaciones, seguridad perimetral y otros servicios corporativos, son divididas de tal forma que el equipo pueda garantizar la seguridad de la información en los servicios que se prestan.

6.1.3 Contacto con Autoridades

EL CONSEJO PROFESIONAL mantiene un contacto adecuado con autoridades pertinentes, en seguridad de la información, las cuales pueden ayudar y guiar a la organización, en la gestión de incidentes de seguridad de la información dentro de la empresa. Las principales autoridades en materia de seguridad en el país, Colombia, son las siguientes:

- Grupo de respuestas a Emergencias Cibernéticas de Colombia, ColCERT, Gobierno. http://www.colcert.gov.co/index.php
- Centro Cibernético Policial, CCP - Policía. http://www.ccp.gov.co

El Coordinador de Seguridad de la Información y Protección de Datos deberá gestionar y mantener las relaciones con la CCP, y con las demás instituciones si así lo considera y previa autorización del presidente / Secretaria Ejecutiva del área de Tecnologías de la Información y Telecomunicaciones.

6.1.4 Contacto con grupos de Interés especial

Por parte del área de Tecnologías de la Información y Telecomunicaciones, se debe tener una relación activa y apropiada con grupos especializados en el campo de la seguridad informática y tecnologías de la información (TI), como foros, grupos, asociaciones, empresas, entre otros, que mantienen actualizado el panorama y tendencias de la seguridad de la información y TI.

El Coordinador de Seguridad de la Información y Protección de Datos deberá liderar, gestionar y mantener las relaciones con grupos de interés que así lo considere en materia de seguridad informática. Esto se hará con el objetivo de generar espacios donde se compartan conocimientos, charlas o conferencias educativas en materia de seguridad informática o tecnología para los usuarios finales.

6.1.5 Seguridad de la Información en la Gestión de Proyectos

La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto, por tanto, los líderes de proyectos deberán presentar o dar a conocer los nuevos proyectos con anticipación al SGSI, para que este pueda realizar un respectivo análisis de riesgos, así como las sugerencias pertinentes en materia de seguridad de la información para los mismos.

6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO

Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

6.2.1 Política para Dispositivos Móviles.

a) No es permitido el uso de dispositivos móviles personales tales como portátiles, smartphones, tabletas y otros relacionados, para el desarrollo de actividades laborales a través de los sistemas de información dispuestos por el área Tecnologías de la Información y Telecomunicaciones de la compañía.

b) Los miembros de Junta Directiva, Presidencia, secretarios y Coordinadores pueden hacer uso de dispositivos móviles personales y corporativos, tales como portátiles, smartphones, tabletas y otros relacionados, para las actividades personales y empresariales. Los mismos deben velar por la seguridad de la información de los dispositivos móviles y su información contenida.

c) El uso de dispositivos móviles personales dentro de la organización es permitido únicamente para fines personales y en los casos de emergencias o fuerza mayor.

d) Está prohibido el almacenamiento de información del CONSEJO PROFESIONAL MVZ privada en dispositivos móviles personales en cualquier formato ya sea texto, imagen, audio y/o video.

e) Se prohíbe la captura de imagen, audio y/o video de la infraestructura interna del edificio, zonas y oficinas, afiliados, funcionarios, y personas que se encuentren dentro de las instalaciones a través de dispositivos móviles, Smartphone, tabletas, IPad y cámaras, sin previa autorización de los coordinadores y directores del área de Talento Humano.

6.2.2 Teletrabajo

Especificar que EL CONSEJO PROFESIONAL MVZ adopta el modelo de trabajo en casa en lugar de teletrabajo, el cual no requiere de la presencia física del trabajador en la entidad, y en donde los suministros de puestos de trabajo, eléctricos y de conexión a internet son aportados por el empleado para realizar una conexión a la red de la organización.

evaluar la reglamentación y diferencias de “trabajo en casa” y “trabajo remoto” y determinar cuál se aplica a EL CONSEJO PROFESIONAL MVZ.

Cuando se requiera realizar labores de teletrabajo o actividades laborales que requieran conexión remota, el líder del área o proceso debe evaluar esta modalidad de trabajo para su empleado y aprobar el acceso de conexión VPN, indicando el tiempo por el cual se requiere la conexión remota para el desarrollo de las actividades laborales, o si se requiere el acceso conforme a las obligaciones contractuales.

Las conexiones remotas a la red corporativa, acceso de conexión VPN, solo se dan a usuarios que por su labor o rol en EL CONSEJO PROFESIONAL MVZ requieren de este tipo de servicios. El acceso se brinda para la realización de actividades laborales desde sitios alternos con conexión a internet, siempre bajo el control de acceso y las autorizaciones pertinentes. La responsabilidad de las acciones ejercidas en el desarrollo de las actividades de trabajo remoto o teletrabajo recaen estrictamente en el usuario y la coordinación o área a la que pertenece.

En los casos que el acceso y procesamiento de la información sea mediante la modalidad de acceso remoto o teletrabajo, los responsables de estas actividades deberán dar cumplimiento a las buenas prácticas, condiciones y restricciones definidas entorno a la seguridad de la información, para lo cual se deben tener en cuenta las siguientes disposiciones.

a) Se deben utilizar los servicios de VPN para acceso a y escritorio remoto corporativos como medio de conexión seguro a la red empresarial, es necesario el diligenciamiento del formulario de solicitud de servicios de TI, para obtener autorización y acceso a estos servicios.

b) No está permitido el uso de herramientas no corporativas oficiales para la conexión a la red empresarial como son Anydesk, Team Viewer ya que estas herramientas pueden llegar a constituir un riesgo a nivel de seguridad.

c) Contar con una Seguridad física y de comunicaciones adecuadas en el sitio de conexión remota.

d) Se debe tener un Control de accesos a información o recursos obtenidos de manera remota.

e) Hacer uso de software licenciado; en los casos que sea aplicable.

f) Solo Utilizar Uso de equipo corporativos o personales para la utilización de VPN (No utilizar equipo de terceros café internet, universidades, entre otros)

g) Contar con un antivirus licenciado y actualizado en los dispositivos de conexión remota o equipos de cómputo.

h) Los dispositivos de conexión remota y equipos de cómputo deben estar actualizados en lo posible con los últimos parches de seguridad.

i) Una vez se termine la jornada laboral o las actividades laborales se debe verificar la desconexión de la VPN.

j) No se debe utilizar redes inalámbricas gratuitas de cualquier zona pública. Estas conexiones no poseen medidas de seguridad y cualquier persona conectada a la misma puede interceptar el tráfico e incluso manipularlo.

k) Contar con una suite de office licenciado en caso de ser necesario, o se recomienda utilizar la plataforma de Google Workspace.

l) Cumplir con la política de contraseñas seguras. Es necesario revisar y fortalecer las contraseñas, recuerde que lo ideal es que sean mínimo de 10 caracteres alfanuméricos y con caracteres especiales, no deben ser relacionadas con algo que lo pueda identificar, por ejemplo: fechas de nacimiento, nombres de sus hijos, mascotas, etc con el fin de no ser víctimas de técnicas de ingeniería social; las cuales debe estar cambiando de forma periódica y evitar el almacenamiento en los navegadores.

m) Utilizar navegadores Google Chrome, Firefox actualizados.

n) No utilizar medios de almacenamiento USB en los dispositivos de conexión remota para la transferencia de información, se debe utilizar Almacenamiento en Cloud.

o) En lo posible tener una conexión de Internet de mínimo de 5MB, para un buen funcionamiento de las aplicaciones.

p) Cuando se encuentre conectado a la VPN usar el navegador web solo para las actividades laborales.

q) En caso de presentarse anomalías, eventos o incidentes que puedan afectar los sistemas o la información de la compañía, se debe comunicar al área de seguridad de información por medio de los canales de comunicación establecidos (Otros, Correo, etc.), notificando lo sucedido para tomar las medidas necesarias para proteger los sistemas y/o salvaguardar la información.

7. SEGURIDAD DE LOS RECURSOS HUMANOS

7.1 ANTES DE ASUMIR EL EMPLEO

7.1.1 Selección

El área de Talento Humano debe hacer verificación de antecedentes de los candidatos al empleo, contratistas y terceros, en concordancia con las regulaciones, las leyes relevantes y la ética organizacional, siendo afín a los requerimientos el CONSEJO PROFESIONAL , además de la clasificación de la información a la cual se va a tener acceso y los tipos de riesgos percibidos, así como la protección de la información de la privacidad, del tratamiento de los datos personales, la disponibilidad de referencias, verificación de la hoja de vida, confirmación de las calificaciones o certificados académicos y profesionales declarados.

Es importante también que se asegure de que los candidatos tengan las competencias para desempeñar los cargos a los que aspiran, y si son cargos de importancia los mismos sean confiables para desempeñar el rol al que aspira.

7.1.2 Términos y condiciones del empleo

Como parte de obligación contractual, empleados, contratistas y terceros deben aceptar. Firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones del CONSEJO PROFESIONAL para la seguridad de la información.

Así mismo Talento Humano deberá hacer firmar a todos los empleados y contratistas a los que se brinde acceso a información confidencial acuerdos de confidencialidad y no divulgación, antes de asumir el cargo o roles establecidos.

7.2 DURANTE LA EJECUCIÓN DEL EMPLEO

7.2.1 Responsabilidades de la Dirección

Las áreas a través del área Talento Humano y Tecnologías de TI y Telecomunicaciones y otras áreas exigirá que los empleados, contratistas y usuarios de terceras partes que apliquen la seguridad

según las políticas y los procedimientos establecidos por la organización, esto se realizará mediante los contratos tanto laborales como con otros terceros.
La Presidencia y Secretaria Ejecutiva se comprometen en apoyar al SGSI a través de una ordenanza para el cumplimiento de las presentes políticas de seguridad de la información. Se compromete en apoyar los programas educativos en materia de seguridad de la información para los colaboradores tales como seminarios, conferencias, espacios de charlas y difusión a través de los diversos canales de comunicación.

7.2.2Toma de Conciencia, educación y Formación en seguridad de la información

a) El Coordinador de Seguridad de la Información y Protección de Datos realizará junto con el área de comunicaciones constantemente campañas de concientización por medios como correos electrónicos, publicaciones, mensajes, etc. También velará porque los nuevos funcionarios y contratistas reciban inducción en seguridad de la información al ingresar a la entidad.

b) En todos los niveles de la organización se debe contar con el grado de conocimiento apropiado, que garantice la concientización y habilidades que permitan minimizar la ocurrencia y la severidad de incidentes de Seguridad de la Información. Cualquiera de los Colaboradores está en el derecho de solicitar asesorías educativas en materia de seguridad de la información al profesional SGSI en el momento que así lo requiera.

c) Se realizará capacitación a los funcionarios sobre Seguridad de la información, amenazas informáticas, tipos de ataques, ingenierías sociales y relacionadas por medio de charlas informativas, cursos virtuales, conferencias y noticias sobre seguridad de la información y seguridad informática.

7.2.3 Proceso disciplinario

Dentro de la documentación del proceso disciplinario se debe incluir un mecanismo de disuasión para prevenir que los empleados o colaboradores violen las políticas y controles de seguridad de la información.

Todo incidente de seguridad en los activos de información y/o en el manejo de la información en los que estén involucrados usuarios y/o colaboradores, internos o externos, debe ser investigado por Control Interno y Jurídica, conjuntamente con el equipo de seguridad, para establecer responsabilidades y determinar las sanciones correspondientes.

En los incidentes de seguridad de la información reportados al proceso de Seguridad de la Información en los que estén involucradas terceras partes, serán informados por éste al área Jurídica y al área directamente relacionado para el inicio de las acciones pertinentes.

7.3 TERMINACIÓN Y CAMBIO DE EMPLEO

7.3.1Terminación o cambio de responsabilidades de empleo

El área de Talento Humano es la encargada de realizar las gestiones necesarias para los traslados o finalización de las relaciones laborales. Así mismo estos deberán recordar las cláusulas de confidencialidad de la información posterior a la terminación laboral.

Talento Humano es responsable de generar las comunicaciones respectivas para informar a las otras áreas de los traslados o retiros de los funcionarios para que se proceda con las gestiones pertinentes para la seguridad de la información, tales como retiro de permisos, accesos y demás gestiones.

8. GESTIÓN DE ACTIVOS.

8.1 RESPONSABILIDAD POR LOS ACTIVOS

8.1.1 Inventario de activos.

Todos los computadores, servidores y portátiles de la compañía comprados o alquilados deberán ser registrados en el inventario de equipos de cómputo, en donde se registre información relacionada con: hardware, sistema operativo y software base instalado, fecha de compra o alquiler, especificaciones generales, etc. Esta información deberá ser consignada una vez hayan sido recibidos los equipos en cuestión; la actualización del inventario de equipos se llevará a cabo cada vez que se realice cualquier tipo de modificación de software o hardware sobre los mismos.

El mantenimiento físico de todos los equipos el CONSEJO PROFESIONAL, las revisiones de mantenimiento de software, revisión de la vigencia de licencias y software no autorizado instalado se realizará anualmente y estará a cargo del área de Tecnologías de la Información y Telecomunicaciones.

El área de Tecnologías de la Información y Telecomunicaciones realizará el mantenimiento de equipos de usuario, servidores y redes.

Adquisición y asignación de equipos de usuario

La adquisición y asignación de equipos la realizará el área Administrativa y los entregará al área de Tecnologías de la Información y Telecomunicaciones para su configuración y entrega al funcionario.

Los equipos de cómputo tendrán instalados única y exclusivamente los aplicativos y/o programas debidamente licenciados y aprobados teniendo en cuenta las funciones del usuario que lo utilizará. Adicionalmente se deben aplicar todas las restricciones y realizar las instalaciones de software

correspondientes incluyendo el Antimalware. Hasta tanto el equipo no se encuentre en condiciones adecuadas para su uso, el usuario no podrá utilizarlo.

Activos críticos

El Coordinador de Seguridad de la Información y Protección de Datos realizará el levantamiento de información de los activos críticos de la entidad en conjunto con los líderes de los procesos, así como de los requerimientos de integridad, confidencialidad y disponibilidad de dichos activos, esto en el proceso de análisis de impacto al negocio y en la gestión del riesgo.

Los colaboradores deberán identificar activos de información no tangibles tales como documentos, archivos de bases de datos, hojas de cálculo, etc. que se encuentren en sus equipos de cómputo asignados y deberán propender por proteger su integridad, confidencialidad y disponibilidad.

8.1.2 Propiedad de los activos

Los activos del inventario deberán contar con un propietario, el cual tendrá acceso en el uso de los mismos. Los propietarios son responsables por mantener y usar los activos en forma correcta. El proceso de Seguridad de la Información deberá acompañar a los propietarios de activos de información con el fin de que los activos estén inventariados, clasificados y protegidos apropiadamente.

8.1.3 Uso aceptable de los activos

Uso general

Los activos de información pertenecen a el CONSEJO PROFESIONAL y el uso de los mismos debe realizarse exclusivamente con propósitos laborales. Toda solicitud realizada al área de Tecnologías de la Información y Telecomunicaciones respecto al uso de los activos debe ir en el formulario de Solicitud de Servicios de Tecnología.

- La información, considerada como uno de los activos más valiosos, que los funcionarios manejan dentro del desarrollo de sus labores diarias debe ser utilizada única y exclusivamente para fines laborales, y no debe ser usada para beneficio propio o de terceros; así mismo, debe ser manejada y protegida de acuerdo al nivel de clasificación definido en las tablas de retención.

- Manejo de la confidencialidad, integridad y disponibilidad: cada funcionario debe realizar sus labores teniendo como principio el evitar la divulgación no autorizada, pérdida o daño de la información; independientemente del medio en que se encuentre, sea físico o electrónico.

- Está prohibido divulgar información de la cual se tenga conocimiento en relación con el ejercicio de las funciones y que no esté destinada al público en general u otros procesos y/o personal internos.

- Las partes externas que por las relaciones contractuales o de cooperación requieran acceso a ciertos activos de información lo podrán tener bajo previa autorización formal de la Presidencia, Secretaría o dirección de proceso relacionado.

Uso de computadores

- Un funcionario solo tendrá asignado un equipo de cómputo y un solo usuario para cada uno de los sistemas que utilice.

- Está prohibido realizar sin autorización copias de la información confidencial perteneciente a el CONSEJO PROFESIONAL, mediante dispositivos de grabación, o a través de cualquier medio de almacenamiento externo (CD, DVD, discos duros externos, memorias USB, etc.). Con el fin de controlar la fuga de información utilizando dispositivos de almacenamiento con puertos USB, se bloquearán los puertos USB y las unidades de CD/DVD de los computadores que posee o administra EL CONSEJO PROFESIONAL. Se exceptúan los funcionarios del área de Tecnologías de la Información y Telecomunicaciones que por sus funciones requieren tener la posibilidad de utilizar estos dispositivos.

  Para no afectar la operación de la organización se deben utilizar las herramientas autorizadas por parte del área de Tecnologías de la Información y Telecomunicaciones, las cuales cumplen con los protocolos de seguridad de la información, como plataformas de almacenamiento cloud, Correo Electrónico, Chat), FTP, Repositorios, Unidades Compartidas.

- Cuando se realicen copias de seguridad diferentes a las que realiza el área de Tecnologías de la Información y Telecomunicaciones para salvaguardar la información, éstas deben ser solicitadas y autorizadas por el líder del proceso y se debe informar al Profesional Administrador SGSI. En el caso de que esta información sea dirigida a un ente de control, la misma debe estar soportada por el requerimiento donde se solicita y se debe entregar con acta o formato de entrega de información indicando el SHA-512 de la información para prevenir la pérdida de la integridad.

- Cuando se realice copia de información a un computador de un funcionario de la entidad, este debe ser informado previa dicha actividad, la copia permanecerá en custodia del área de Tecnologías de la Información y Telecomunicaciones. Si la copia es solicitada, su entrega debe ser autorizada por el secretario o director del funcionario respectivo.

- En caso de ausencia de un funcionario sin reemplazo y de llegarse a necesitar información del computador asignado a éste, se deberá solicitar previa autorización de la secretaria ejecutiva o coordinador del proceso. El acceso a estos archivos debe ser informado al Profesional Administrador SGSI de la Información.

- Se deben tener las precauciones necesarias al comer o beber en el puesto de trabajo para evitar daños al computador, documentos o los elementos de trabajo.

- Está prohibido intercambiar partes entre computadores (mouse, teclados, monitor, etc.), sin previo consentimiento del área de Tecnologías de la Información y Telecomunicaciones y dejar los registros por correo electrónico o por escrito de dichos cambios.

- No está permitido almacenar en el disco duro del computador, ni en las carpetas de red, archivos (música, videos, fotos, programas y otros) que violen las leyes de propiedad intelectual y que no sean a fin con los propósitos el CONSEJO PROFESIONAL.

- Los funcionarios deben comunicar inmediatamente solo al área de Tecnologías de la Información y Telecomunicaciones toda vulnerabilidad u operación sospechosa que se encuentre en los sistemas, manifestación de malware, virus o programas sospechosos e intentos de intromisión en los sistemas (ej. Bloqueo constante del usuario en los sistemas), no deben revelar este tipo de información ni interna o externamente.

- Informar al presidente, secretario o director respectivo y al proceso de Seguridad de la Información cuando se tenga conocimiento de cualquier asunto interno o externo que pueda afectar la confidencialidad, integridad o disponibilidad de la información del CONSEJO PROFESIONAL y perjudicar la imagen de la entidad ante los entes de control y vigilancia o cualquier otro.

- Está prohibido leer documentos que se especifiquen expresamente o según la clasificación de la información como confidenciales, dirigidos a otros procesos o funcionarios.

- El traslado y movimiento de equipos (excepto los portátiles) debe ser realizado por el área de Tecnologías de la Información y Telecomunicaciones.

Uso de Internet

- El servicio de Internet está habilitado por defecto para todos los funcionarios que por la naturaleza de su labor requieran el uso de esta herramienta. El acceso a sitios que no se requieren normalmente para las funciones laborales estará bloqueado si se encuentran en las siguientes categorías.

  - Sitios para adultos (Pornografía, Sexo explícito, Citas)
  - Violencia, armas, agresión
  - Drogas, alcohol y tabaco
  - Audio y video (radio, streaming, sitios de video del tipo YouTube o Video, TV en vivo).
  - Entretenimiento (Humor, cocina, mascotas, astrología, etc....)
  - Juegos de cualquier índole
  - Chats, blogs, página de contactos, etc.
  - Redes sociales (Facebook, Twitter, Youtube, Whatsapp)
  - Sitios Maliciosos / ciberdelincuencia, Phishing, Spam.
  - Sitios que permitan acceder a software pirata y/o malware
  - Sitios de descargas de software y Freeware ◦ Sitios de correos personales (outlook, mail, yahoo, etc)

- Sitios de almacenamiento en la nube o transferencia de archivos. (Onedrive, WebTransfer, etc).

- El personal que por sus funciones requiera acceder a alguna página o categoría debe solicitar a su Coordinador la autorización diligenciando el formulario solicitud de permiso de servicios el cual debe ser aprobado por el proceso de seguridad para la aplicación de los permisos.

- La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable, si se requiere descargar archivos superiores a 300MB se debe solicitar a Tecnologías de la Información y Telecomunicaciones que realice la descarga para no afectar la navegación de los demás usuarios. No está permitido descargar información que pueda atentar contra las leyes de propiedad intelectual y derechos de autor.

- Los profesionales y Auxiliares del área de Tecnologías de la Información y Telecomunicaciones que lo requieran tendrán acceso a las categorías Audio y video (videos y tutoriales), Chats, blogs, página de contactos, foros, Redes sociales (sólo para casos particulares), asimismo, podrán realizar descargas mayores a 300Mb tanto para ellos como para los otros funcionarios que lo requieran, siempre que sea con propósitos alineados a los objetivos del CONSEJO PROFESIONAL y el área de Tecnologías de la Información y Telecomunicaciones. El uso que se le dé a estos sitios y las precauciones de seguridad son responsabilidad de cada funcionario del proceso de Administración de Infraestructura Tecnológica y los mismos serán supervisados por el proceso de Seguridad de la Información.

- A los activos tipo equipos servidores no está permitido la salida a Internet, exceptuando el servidor de actualizaciones de Microsoft y los que por los servicios que prestan lo requieran. Los servidores que deban ser accesibles desde Internet deberán estar en una Zona Desmilitarizada, con acceso limitado a la LAN.

- Los informes de navegación y posibles intrusiones, generados por los equipos y herramientas de seguridad perimetral deben ser generados y analizados periódicamente o cada vez que se detecte un incidente grave de seguridad.

Uso de correo electrónico y mensajería instantánea

- El servicio de correo electrónico tiene como objeto la comunicación a nivel corporativo, con los funcionarios de la misma entidad, proveedores, prestadores o cualquier tercero que tenga relación con EL CONSEJO PROFESIONAL. La información que se envíe por este medio es propiedad del CONSEJO PROFESIONAL MVZ y por ende cualquier acceso o investigación a ésta, se realizará con autorización expresa de la Presidencia y la secretaria ejecutiva de CONSEJO PROFESIONAL.

- Los correos electrónicos enviados y que tengan documentos adjuntos deberán tener un tamaño máximo de veintiséis (26) megabytes (MB), en caso de superar este límite se deben

enviar los adjuntos en más de un correo, comprimir la información en archivo .zip o consultar alternativas con el área de Tecnologías de la Información y Telecomunicaciones.

- Está prohibido el envío de archivos tipo MP3, WAV, EXE, LNK archivos de video o cualquier otro tipo de archivo que viole la propiedad intelectual, los derechos de autor, la dignidad humana o que genere daño o perjuicios a terceros.

- El correo electrónico corporativo es para uso laboral, no está permitido darle uso para fines personales y comerciales como promoción de productos, rifas y suscripciones sin autorización de la Presidencia, la secretaria general o la Coordinación de Sistemas.

- El correo corporativo no debe ser usado para el envío de cadenas ya que pueden traer archivos adjuntos de gran volumen o virus ocultos.

- No se permite el envío de correos con contenido que atente contra la integridad humana de las personas o instituciones, tales como: pornográfico, chistes, religiosos, terroristas, hackers, racistas, políticos o cualquier contenido que represente riesgo de virus; código malicioso, etc.

- Las credenciales de acceso a las cuentas de correo electrónico corporativo asignadas a los usuarios son intransferibles no se pueden compartir los accesos.

- Los correos electrónicos deben contener la sentencia de confidencialidad con el siguiente contenido: “AVISO LEGAL: La información contenida en este mensaje electrónico, tiene carácter privado y confidencial. Solo puede ser utilizado por el destinatario. Cualquier copia o distribución, su reenvío total, parcial o su uso sin contar con expresa autorización de su autor, está totalmente prohibida y sancionada por la ley. Si por algún motivo usted ha recibido el presente mensaje electrónico por error a su correo electrónico, por favor elimínelo y comuníquelo al remitente. El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida esta comunicación, antes de que llegue a su destinatario, estará sujeto a las sanciones penales correspondientes, al igual que el que en provecho propio o ajeno o con perjuicio de otro, divulgue o emplee la información contenida en la misma. Todas las ideas y reflexiones expresadas en el presente mensaje electrónico corresponden al remitente del mismo y NO representa la posición oficial de EL CONSEJO PROFESIONAL.

- Los usos de programas de mensajería instantánea de carácter público no están permitidos, ya que representan elementos de exposición pública y evaden los controles perimetrales.

- Si un funcionario por sus funciones necesita tener habilitado el correo electrónico personal en su puesto de trabajo, debe solicitar a su coordinador que realice la solicitud al área de Tecnologías de la Información y Telecomunicaciones por medio del Formato Solicitud de Servicios de Tecnología, con autorización del líder de proceso quien debe evaluar el impacto y determinar si realizar o no la habilitación. Asumiendo los riesgos que este hecho conlleva.

Servicios de red

- Los recursos de red que ha dispuesto el CONSEJO PROFESIONAL, tales como Archivo Central, Carpetas compartidas ftp, etc., deben ser utilizados para el almacenamiento de información con propósitos laborales; información como material pornográfico, videos, películas, música, fotos, etc. están prohibidos de almacenar y de encontrarse serán eliminados sin previo aviso.

- Está prohibido crear carpetas compartidas en la red por los funcionarios, esto sólo debe ser realizado por personal del área de Tecnologías de la Información y Telecomunicaciones.

- El área de Tecnologías de la Información y Telecomunicaciones realiza periódicamente copias de seguridad a la información almacenada en el Archivo Central. Los Backups de otras unidades o por demanda se deben solicitar a través de la herramienta de mesa de ayuda.

Uso de las aplicaciones corporativas

- Los registros de las operaciones realizadas en los sistemas serán almacenados en el sistema y sólo algunos funcionarios del área de Tecnologías de la Información y Telecomunicaciones tendrán acceso permanente a ellos. Si se requieren consultas de estos registros de parte de entes de control y el área de Control Interno estos registros podrán ser entregados sin autorización formal, pero con acta de recibido, en cualquier otro caso debe ser solicitado formalmente y entregado por el Coordinador de Tecnologías de la Información y Telecomunicaciones.

- Las aplicaciones corporativas se deben usar para su propósito y las actividades corporativas, no se debe extraer información de las aplicaciones corporativas con fines personales o en beneficio propio o de terceros no autorizados.

- El acceso a las aplicaciones corporativas está definido por usuario y contraseña para cada colaborador, estos deben propender por proteger sus credenciales de acceso y no deben compartir estos datos con otros colaboradores o terceros.

Uso de la red inalámbrica

- La entidad tendrá una red de invitados para conexión inalámbrica a Internet de equipos de visitantes que lo soliciten, esta conexión permite navegación de uso general y cuenta con restricciones de acceso a sitios de categorías que representan amenazas para la organización, puede ser accedida desde equipos portátiles y dispositivos móviles en iguales condiciones, esta red será aislada de la red LAN, MPLS y DMZ, es una red únicamente de acceso a internet.

- El equipo de seguridad perimetral debe estar configurado para realizar sobre las redes inalámbricas revisión de anti-virus y anti-spyware/anti-malware, así mismo debe tener

habilitado IDS/IPS, y bloqueo de descargas P2P y aplicaciones categorizadas en el listado de categorías bloqueadas.

- Las redes inalámbricas corporativas que permitan el acceso a la red LAN de la entidad deben ser administradas por el área de Tecnologías de la Información y Telecomunicaciones, tener filtrado por MAC y no difundir el nombre de la red. Serán configurada a los funcionarios que la requieran y hagan la solicitud formal.

- En caso de detectar actividad anómala o sospechosa a través de estas redes se debe monitorear y alertar al Profesional Administrador SGSI y al Coordinador de TI.

- Las claves de acceso a las redes inalámbricas deben ser cambiadas cada 6 meses o antes si se sospecha que se han divulgado las claves.

8.1.4 Devolución de activos

- El funcionario es responsable de realizar la devolución de activos y la información con el fin de obtener las firmas del Acta de entrega de cargo en señal de paz y salvo a satisfacción por parte de los procesos respectivos.

- El área de Talento Humano validará dicha devolución de manera previa al trámite del pago de liquidación.

- La tarjeta de acceso físico debe ser devuelta al área de Tecnologías de la Información y Telecomunicaciones, donde se retirarán los accesos.

- El funcionario o terceras partes no podrán extraer, secuestrar mediante cifrado ni borrar información de propiedad el CONSEJO PROFESIONAL.

8.2 CLASIFICACIÓN DE LA INFORMACIÓN.

8.2.1 Clasificación de la información.

El área de Administrativa realizará una vez al año la revisión de las Tablas de Retención Documental de la entidad, y realizará la actualización cuando lo considere necesario.

- La información del CONSEJO PROFESIONAL se clasificará en términos del valor, de los requisitos legales y de su sensibilidad e importancia para el CONSEJO PROFESIONAL de acuerdo al esquema de clasificación adoptado por la Entidad en este documento; en el cual se definen tres (3) niveles de clasificación: Pública, Interna y Confidencial. Esta política establece un esquema de clasificación de información de la siguiente forma.

Tabla 1. Categorías de clasificación de la información

Clasificación	Características
Pública	Esta información ha sido aprobada por EL CONSEJO PROFESIONAL MVZ para su diseminación pública. Son también públicos los datos calificados como tal según la ley y todos aquellos que no sean semiprivados o privados. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas. Se espera que en casi todas las circunstancias la divulgación de esta información no cause ningún daño a EL CONSEJO PROFESIONAL. Ejemplos: Boletines de noticias, informes de prensa, valores pagados entre otros. **Almacenamiento**: Se almacenará una copia dentro de la entidad como Backups.
Interna	Se espera que la revelación o divulgación de esta información, no cause daños serios a EL CONSEJO PROFESIONAL, y su acceso es libre para los funcionarios de la Entidad a través de la red de la entidad y/o intranet. Está cubierta por los acuerdos de confidencialidad firmados por los funcionarios como parte de su contrato laboral y por los terceros como parte de los contratos respectivos. La información cuyo nivel de confidencialidad no haya sido clasificado se considerará **Interna.** Ejemplos: Directorio de la organización, código de ética y buen gobierno, reglamento interno de la entidad, entre otros. **Almacenamiento**: Se puede almacenar en cualquier medio que forme parte de la infraestructura Interna (Informática o Física) de la entidad, para su almacenamiento externo o salida se debe realizar un análisis de riesgos e implementar los controles requeridos.
Confidencial	A este tipo de información sólo podrán tener acceso los funcionarios del proceso propietario de la información y de otros procesos a los que se les autorice por su cargo o sus funciones, es de uso exclusivo interno de la organización y su divulgación se considerará un incumplimiento a los acuerdos de confidencialidad firmados por los funcionarios como parte de su contrato laboral y por los terceros como parte de los contratos respectivos. Ejemplos: Datos personales o reportes bases de datos de los sistemas de información **Almacenamiento**: Se mantendrá almacenada en los medios designados por el propietario de la información bajo los lineamientos que este dé, Tecnologías de la Información y Telecomunicaciones apoyará la implementación de los controles que sean necesarios. Se deben tener las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

- El uso que se dará a los datos personales (en especial los datos sensibles) de los usuarios, su tratamiento, los derechos del usuario con respecto a la misma, la autorización de su uso, divulgación o entrega estarán amparados por la política de tratamiento de datos personales del CONSEJO PROFESIONAL bajo la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.

- La información clasificada como Confidencial, no debe ser revelada en ningún ámbito personal como en el hogar, en sitios públicos ni en reuniones sociales, entre otros.

- La información debe ser protegida de acuerdo a su nivel de clasificación, sin importar donde resida, su forma, que tecnología fue usada para manejarla y el propósito para el que ella existe. Esta clasificación debe ser realizada por el Propietario o propietarios de la información, teniendo en cuenta las leyes que regulen la misma. Se debe revisar este nivel de clasificación al menos una vez al año al actualizar las tablas de retención documental.

- La información que se reciba a través de terceros para usarla por el CONSEJO PROFESIONAL debe ser clasificada de acuerdo a la tabla de clasificación de información, y debe ser protegida por los funcionarios que la administran de la misma forma que se haría con la perteneciente a el CONSEJO PROFESIONAL.

- Cuando la información del CONSEJO PROFESIONAL sea utilizada, procesada o accedida por terceros, es obligación de la tercera parte respectiva conocer y prestar el cuidado y protección de acuerdo a la clasificación establecida por el CONSEJO PROFESIONAL.

- La nómina es de carácter confidencial y propiedad del área de Talento Humano por lo tanto no se podrá revelar información relacionada con esta a ningún funcionario o tercero sin autorización del mismo.

- Se entenderá por Dato Personal cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables; la información personal o datos personales son confidenciales, sean privados o semiprivados. Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero, crediticio, comercial, de servicios o proveniente de terceros países.

- Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros debidamente autorizados.

8.2.2 Etiquetado de la información

Dentro del CONSEJO PROFESIONAL el etiquetado de información sólo se contempla en los casos explícitos de Copias de seguridad, en donde las copias se etiquetan de la siguiente manera:

- BD#: Hace referencia a bases de datos acompañado del # es el consecutivo del disco.
- AC#: Hace referencia al archivo central acompañado el correspondiente consecutivo #.
- US#: Hace referencia a los usuarios acompañados del respectivo número consecutivo #.
- ANEXOS#: hace referencia a los anexos o Diferente Información no clasificada.

8.2.3 Manejo de Activos

En referencia a la información, el manejo de los activos se realizará bajo los lineamientos que dé Talento Humano por medio del área Administrativa en políticas, circulares y demás comunicaciones internas que se emitan. Cada área es responsable por los activos de información bajo su gestión y custodia.

8.3 MANEJO DE MEDIOS

Se considera en este apartado de políticas el mitigar la divulgación, modificación, retiro o destrucción no autorizada de información contenida en medios.

8.3.1 Gestión de medio removibles

Está prohibido realizar sin autorización copias de la información confidencial perteneciente a el CONSEJO PROFESIONAL, mediante dispositivos de grabación, o a través de cualquier medio de almacenamiento externo (CD, DVD, discos duros externos, memorias USB, etc.). Con el fin de controlar la fuga de información utilizando dispositivos de almacenamiento con puertos USB, se bloquearán los puertos USB y las unidades de CD/DVD de los computadores que posee o administra el CONSEJO PROFESIONAL. Se exceptúan los funcionarios del área de Tecnologías de la Información y Telecomunicaciones que por sus funciones requieren tener la posibilidad de utilizar estos dispositivos.

Cuando se requiera se debe solicitar autorización al área de Tecnologías de la Información y Telecomunicaciones para el retiro de los medios de la organización y llevar registro de esta actividad.

Si la integridad o confidencialidad de los datos o información contenida en medio removibles, tales como USB o Discos duros portables, se considera importante y de alto valor para el CONSEJO PROFESIONAL, se deben utilizar técnicas de criptográficas para la protección de los datos e información.

Los medios removibles de la organización deben estar inventariados y llevar un registro de uso para evitar la pérdida o fuga de información.

8.3.2 Disposición de los medios

- La información contenida en medios que ya no se utilizaran debe ser eliminada de forma segura, para ello se hará cargo el área de Tecnologías de la Información y Telecomunicaciones.

- Los medios que ya no se utilizarán u obsoletos no podrán ser vendidos o donados a externos por ningún motivo.

- Los medios que se dispongan para reutilización tales como discos duros, memorias USB, discos extraíbles deberán ser cifrados antes de ser formateados de forma segura, para ello se hará cargo el área de Tecnologías de la Información y Telecomunicaciones.

- Todos los medios que cumplieron su vida útil deberán ser desechados de forma segura, para ello deberá encargarse el área de Tecnologías de la Información y Telecomunicaciones.

8.3.3 Transferencia de Medios

Los medios se consideran dispositivos o mecanismos en los cuales se almacenan datos y/o información de la organización. Se considera el papel, cintas, discos duros, tarjetas extraíbles, CD/DVD, USB o Pendrives, y entre otros relacionados.

- Los medios físicos de almacenamiento como CD/DVD, Discos duros, Discos Extraíbles, memorias, y otros, que contienen información de tipo Confidencial deberán ser protegidos contra acceso no autorizado, uso indebido o corrupción durante el transporte o transferencia de cualquier forma entre parte interesadas.
  cifrado

- Será el dueño de la información quien clasifique la información y así mismo solicite al área de tecnología a través de la herramienta de mesa de ayuda los servicios pertinentes para garantizar la Transferencia de dichos Medios.

- Los medios se deben transportar a través de los servicios de mensajería terrestre acordados por la organización. Se debe evitar envíos de medios a través de terceros no autorizados.

- Se debe realizar un adecuado embalaje de los medios que se van a enviar, se debe considerar la duración del tránsito entre las partes interesadas, condiciones del ambiente como la temperatura, polvo o humedad.

- Es importante que se realice el registro del contenido de medios que se envían, duración del tiempo de transferencia a los destinos, así como tiempos de recepción de medio enviado.

- También se incluyen como medios al papel, ya que en los mismos se pueden contener y transportar datos e información.

9. CONTROL DE ACCESO

9.1 REQUISITO DEL NEGOCIO PARA CONTROL DE ACCESO

9.1.1 Política de control de acceso

- Se garantizarán a los funcionarios los accesos definidos para su cargo y los adicionales que le sean solicitados por su coordinador para el cumplimiento de sus funciones.

- Adicionalmente se evaluarán individualmente y se podrán dar accesos que contribuyan a mejorar su desempeño laboral o formación personal siempre y cuando no representen un riesgo para la seguridad de la información de la entidad.

- Los accesos que puedan representar un riesgo para la seguridad de la información serán brindados bajo los controles necesarios y autorizados siempre por el Presidente / Secretaria Ejecutiva, Coordinador o Jefe de área, quienes compartirán con el funcionario la responsabilidad por las consecuencias que puedan ocasionarse a partir del uso de los accesos; esto aplica para accesos al funcionario y para accesos a terceros que solicite el funcionario interventor.

- Para terceros el control de acceso estará regido por las condiciones y cláusulas contractuales y no se podrán extender más allá de la finalización del contrato bajo ninguna circunstancia.

- En caso de eventos y/o incidentes de seguridad de la información se podrán retirar los accesos al o los usuarios involucrados.

- Cada área a través de Directivos o sus Coordinadores son responsables de brindar los accesos a los datos e información gestionados bajo su custodia a los colaboradores bajo su cargo o de otros procesos o externos que por cuestiones contractuales se relacionen.

9.1.2 Acceso a redes y servicios de red

- Se permite a los usuarios y funcionarios el uso de los canales, servicios y recursos de red previamente autorizados para cumplir funciones requeridas por el cargo o para el proceso, realizar solicitudes de gestión en redes y elementos de conectividad para mejorar su desempeño laboral o formación personal siempre y cuando no representen un riesgo para seguridad de la información de la entidad.

- El CONSEJO PROFESIONAL se reserva el derecho de almacenar archivos de registro (conocidos como Logs) de las actividades de los usuarios al hacer uso de la infraestructura

de red, los canales o servicios de internet y revisarlos formal o informalmente por el personal del área de Tecnologías de la Información y Telecomunicaciones.

- Está prohibido el uso de datos/información accesible a través de canales de internet para actividades no relacionadas con el cargo, el abuso de privilegios de usuario para acceder a datos o información sobre la que no se tiene autorización, el espionaje por cualquier medio (electrónico, digital o físico) de las actividades de otros usuarios sin su respectiva autorización y la suplantación de usuarios al ingresar con credenciales ajenos a los asignados por el CONSEJO PROFESIONAL.

- El acceso a red VPN Corporativa está limitada a aquellos usuarios a quienes se les haya autorizado la conexión mediante previo diligenciamiento de solicitud formal de este servicio.

- Las redes inalámbricas corporativas que permitan el acceso a la red LAN de la entidad deben ser administradas por el área de Tecnologías de la Información y Telecomunicaciones, tener filtrado por MAC. Serán configurada a los funcionarios que la requieran y hagan la solicitud formal, dicha configuración será realizada por personal de Tecnologías de la información y Telecomunicaciones.

- Las claves de acceso a las redes inalámbricas deben ser cambiadas cada 6 meses o antes si se sospecha que se han divulgado las claves.

9.1.2.1. Acceso a redes inalámbricas – Wifi Corporativa e Invitados

EL CONSEJO PROFESIONAL MVZ para la conexión de dispositivos móviles dispone de sus redes inalámbricas corporativas seguras. Las cuales se denomina de la siguiente manera:

a) **Red Wifi CORPORATIVA**: Consiste en la red inalámbrica controlada, exclusivamente para los trabajadores el CONSEJO PROFESIONAL, y se aplica únicamente en los casos que no se pueda brindar conexión a red cableada. Esta red cuenta con medidas de seguridad especiales para poder brindar acceso seguro a Internet y a servicios y sistemas de información corporativos.

b) **Red Wifi INVITADOS**: Consiste en la red inalámbrica controlada, para la conexión únicamente a Internet de los usuarios y terceros relacionados con el CONSEJO PROFESIONAL.

- Las redes inalámbricas de la organización deben ser controladas por el área de Tecnologías de la Información y Telecomunicaciones, y el responsable de Seguridad Informática quienes deben aplicar buenas prácticas de implementación y administración de redes inalámbricas seguras.

- Las redes inalámbricas del CONSEJO PROFESIONAL deben contar con control de navegación con el fin de mitigar el riesgo de acceso a sitios no adecuados o peligros tales

como sitios de distribución de software malicioso o malware, pornografía, juegos y apuestas, entre otros relacionados.

- Las redes inalámbricas, tanto **Red Wifi Corporativa** y **Red Wifi Invitados** no se deben utilizar en dispositivos personales móviles tales como portátiles, celulares o Smartphone, Tablet y relacionados. En caso de que se requiera se debe realizar solicitud formal.

- Las redes inalámbricas de tipo **Red Wifi Corporativa** pueden ser configuradas a los empleados que la requieran, en los casos que no se pueda brindar conexión a la red cableada, siempre bajo solicitud, autorización y aprobación formal. La configuración adecuada debe ser realizada por personal de la Coordinación de TIC o Coordinación de Seguridad de la Información. Se debe evitar utilizar este tipo de redes inalámbricas en dispositivos móviles de tipo Smartphone o celulares y Tablet.

- Las redes inalámbricas de tipo **Red Wifi Corporativa** pueden ser utilizadas en dispositivos móviles; bajo revisión previa de seguridad y una correcta configuración por el personal de la Coordinación Infraestructura y Servicios TIC o Coordinación de Seguridad de la Información.

- Las redes inalámbricas de tipo **Red Wifi Invitados** pueden ser configuradas a los empleados que la requieran, bajo solicitud, autorización y aprobación formal. La configuración adecuada debe ser realizada por personal de la Coordinación DE TIC o Coordinación de Seguridad de la Información.

- Las claves de acceso a las redes inalámbricas deben ser cambiadas cada 6 meses o antes si se sospecha que se han divulgado las claves.

9.2 GESTIÓN DEL ACCESO A USUARIOS

9.2.1 Registro y cancelación del registro de usuarios

El registro (creación de cuentas) y la cancelación de usuarios se regirá por lo establecido en el procedimiento Creación y Cancelación de Cuentas y Permisos de Usuarios.

9.2.2 Suministro de acceso de usuarios

- Los accesos de usuarios serán suministrados por el área de Tecnologías de la Información y Telecomunicaciones a cada usuario en particular.

- Una vez el área de Tecnologías de la Información y Telecomunicaciones le informe al funcionario sus datos de acceso según lo establecido en el procedimiento Creación y Cancelación de Cuentas y Permisos de Usuarios la responsabilidad por el uso y cambio de las contraseñas es del funcionario.

- Se tendrán publicados los manuales necesarios para que los funcionarios puedan cambiar sus contraseñas periódicamente.

9.2.3 Gestión de derechos de acceso privilegiado

- Las cuentas con altos privilegios deben ser de uso exclusivo y específico. En lo posible las cuentas de usuario de dominio personal no deben tener altos privilegios, esto se revisará de acuerdo a los requerimientos de los aplicativos.

- Los accesos a aplicativos y privilegios superiores a los definidos para el cargo en el Instructivo de Asignación de Aplicativos deben ser solicitados formalmente, autorizados y documentados mediante el formulario de Solicitud de Servicios.

- Las conexiones a las bases de datos para su administración deben ser autorizadas formalmente mediante el formato definido.

- Los derechos de accesos privilegiados tienen un tiempo de caducidad el cual no puede ser superior a un año, y las cuentas serán monitoreadas periódicamente por parte del área Tecnologías de la Información y Telecomunicaciones.

9.2.4 Gestión de Información de Autenticación Secreta de Usuarios

a) A través de cláusulas de confidencialidad contractuales el o los usuarios (Colaborador, empleado y/o tercero) deben mantener en privado la información secreta para la autenticación. Dentro de la información secreta se encuentran contraseñas, llaves criptográficas, respuestas de preguntas de recuperación de cuentas y otros relacionados.

b) Los usuarios no deben compartir su información secreta para la autenticación temporal que les haya sido suministrada.

c) Después de suministrar a los usuarios la información secreta para la autenticación (contraseñas) de usuario en los equipos de cómputo y otros sistemas, se les solicitará a los usuarios realizar el cambio de la misma por una nueva.

d) Las cuentas de usuario y sus contraseñas son de carácter individual y las primeras son transferibles sólo en situaciones formales de reemplazos o encargos; no está permitido el uso de cuentas de grupo, cuentas genéricas o cuentas compartidas sin autorización del área de Tecnologías de la Información y Telecomunicaciones. La entrega de cuenta de usuario debe ser registrada en el formulario. El colaborador es responsable de custodiar todas las contraseñas que le sean asignadas con el objeto de desarrollar su labor como trabajador el CONSEJO PROFESIONAL, en virtud de lo anterior sus contraseñas son personales y no podrá darlas a conocer o entregarlas a terceros; el sólo hecho de dar a conocer sus contraseñas se tendrá como una falta a sus obligaciones; ahora bien, si esto causa perjuicios al empleador la conducta se catalogará como una falta grave. Se exceptúa de entrega únicamente la clave de solo empleados cuyo registro de transferencia a otra persona debe quedar reportado en el formulario.

e) Las cuentas con altos privilegios no pueden ser compartidas, en caso de requerirse que varios usuarios tengan acceso a privilegios administrativos a nivel del sistema, estos serán otorgados a través de un grupo de usuarios administrativos de sistemas.

f) Las acciones ejecutadas con las cuentas de usuarios, son responsabilidad del propietario de la cuenta.

g) Cada coordinador es responsable de asegurar que sus funcionarios cuenten con las opciones requeridas en los sistemas y aplicativos para el desempeño de su labor y deben solicitar oportunamente los ajustes en los perfiles de usuarios para evitar el uso de claves y usuarios que no correspondan.

h) Las contraseñas de los sistemas de información tendrán una vigencia máxima de 180 días.

i) La longitud de las contraseñas será de mínimo 8 caracteres, deberían contener letras mayúsculas, minúsculas y números (por ejemplo: a-z, A-Z, 0-9).

j) Los sistemas estarán configurados para no permitir contraseñas en blanco.

k) Las contraseñas predefinidas que traen los elementos nuevos tales como Servidores, Bases de Datos, Aplicaciones, Routers, Switches, etc., deben cambiarse antes de poner en producción el equipo.

l) Cuando el área de Tecnologías de la Información y Telecomunicaciones asigne cuentas de usuario y/o asigne una nueva contraseña, el propietario la utilizará solo en el primer inicio de sesión. En el subsiguiente es obligatorio realizar el cambio de contraseña para garantizar que solo él la conoce.

m) Los usuarios serán responsables del uso de las contraseñas que les haya sido suministradas, tanto las generadas por el CONSEJO PROFESIONAL como las que son otorgadas por entidades externas (prestadores de servicios, entidades de control, etc.).

n) Los funcionarios del área de tecnología deben tener actualizado un repositorio cifrado de sus contraseñas corporativas y almacenarlo en una unidad de almacenamiento definida por el área de Tecnologías de la Información y Telecomunicaciones. En caso de requerirse alguna contraseña de urgencia por falla de algún servicio crítico que requiera la asistencia de un tercero y es un requerimiento urgente y/o en horario no hábil y que el funcionario no pueda desplazarse hasta la oficina se realizará el siguiente procedimiento:

- El Coordinador de Tecnologías de la Información y Telecomunicaciones entregara los datos de acceso del servicio al funcionario.

- Una vez obtenida la contraseña por parte de Coordinador de Tecnologías de la Información y Telecomunicaciones o el Coordinador de Seguridad de la Información y Protección de Datos, estos la suministran la fijan directamente en el

servidor para recibir la asistencia tercerizada, de no poderlo ingresar personalmente lo debe suministrar al tercero, teniendo en cuenta que cuando se haya terminado se debe informar a los funcionarios del proceso de infraestructura, para que modifiquen las contraseñas.

g) La responsabilidad del uso de las cuentas del funcionario en caso de llevarse a cabo este procedimiento es del Coordinador de Tecnologías de la Información y Telecomunicaciones o el Coordinador de Seguridad de la Información y Protección de Datos hasta tanto el funcionario se reintegre y se confirme el cambio de sus claves.

9.2.5 Revisión de los derechos de acceso de los usuarios.

a) Una vez al año se revisará que las cuentas de los funcionarios tengan los privilegios establecidos para su cargo, y que los privilegios adicionales que se encuentren hayan sido solicitados formalmente, autorizados y documentados a través de la herramienta de mesa de ayuda.

b) Los privilegios no documentados, no autorizados o vencidos serán retirados hasta tanto se realice el proceso establecido. Las cuentas pertenecientes a usuarios que ya no laboren para el CONSEJO PROFESIONAL o de terceros que finalicen sus actividades, deben ser eliminadas de todos los sistemas y removerlas de todos los grupos a los que pertenecía, o pasadas a estado bloqueado o inactivo si la eliminación puede implicar pérdida de información.

c) El área de Tecnologías de la Información y Telecomunicaciones debe tener actualizada la información de las cuentas de usuarios creadas en los sistemas de información, el estado de cada una y la persona responsable.

9.2.6 Retiro o Ajuste de los derechos de acceso

a) El área de Talento Humano notificará automáticamente por medio de la herramienta de sistematización de procesos al área de Tecnologías de la Información y Telecomunicaciones la fecha de terminación del contrato de un funcionario previamente, para llevar a cabo la inactivación de accesos a más tardar 3 días después de dicha fecha.

b) Para funcionarios con contrato indefinido y OPS se realizará de acuerdo a lo establecido en el procedimiento de creación y cancelación de permisos y accesos de usuarios. El supervisor de contrato es el responsable por realizar de forma oportuna las gestiones correspondientes a la finalización de las actividades de un contratista o la finalización del contrato.

c) Es responsabilidad de los directores o coordinadores notificar al área de Talento Humano el retiro o ausencia temporal por vacaciones, licencias o incapacidad prolongada de cualquier funcionario. de Talento Humano debe informar al área de Tecnologías de la Información y Telecomunicaciones esta situación y si tiene o no reemplazo para inactivar el usuario en los sistemas que corresponda.

9.3 RESPONSABILIDADES DE LOS USUARIOS

9.3.1 Uso de información de autenticación secreta

a) A través de cláusulas de confidencialidad contractuales el o los usuarios (Colaborador, empleado y/o tercero) deben mantener en privado la información secreta para la autenticación. Dentro de la información secreta se encuentran contraseñas, llaves criptográficas, respuestas de preguntas de recuperación de cuentas y otros relacionados.

b) Los usuarios no deben compartir su información secreta para la autenticación temporal que les haya sido suministrada.

c) Está prohibido almacenar datos de acceso de autenticación secreta (contraseñas) en medios no seguros, tales como papel, texto plano.

d) Es importante que el usuario cambie periódicamente sus contraseñas, emplee mecanismo propio que le permitan recordar las contraseñas de manera fácil y segura.

e) No utilice datos personales como fecha de nacimientos, número de identificación y otros parecidos en las contraseñas. Incluya en las contraseñas letras mayúsculas y minúsculas, números y para mayor seguridad caracteres especiales tales como % & $ ” (/) ? ¡ ! + * . ; - _ e incluso espacios en blanco.

9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

9.4.1 Restricción de acceso a la información

Se deben seguir los lineamientos indicados en la presente política sobre control de acceso a activos de información y sistemas. La información se restringe a partir de los medios de almacenamiento, así como las barreras físicas, lógicas y por software a través de roles definidos que se generan en todos los elementos que componen los sistemas de información del CONSEJO PROFESIONAL.

9.4.2 Procedimiento de Ingreso seguro

a) Los usuarios para el inicio de sesión en los diversos sistemas no se visualizará la contraseña, ni otros datos de información secreta de autenticación.

b) Los procesos de acceso a sistemas de información del CONSEJO PROFESIONAL están parametrizados a través de directorio activo con el cual se validan datos de autenticación para acceso y roles definidos de acuerdo al usuario que se autentica.

c) El dominio estará configurado para que se deba enviar el comando Ctrl+ Alta + Supr para iniciar sesión en los equipos.

9.4.3 Sistema de gestión de contraseñas.

a) En lo posible las aplicaciones deberán realizar la autenticación contra el servidor de directorio activo de la organización. Se justificará la autenticación local en los casos en que no sea posible la integración con el LDAP o la migración de usuarios.

b) Los usuarios podrán realizar los procesos de gestión de contraseña a través de la herramienta de mesa de ayuda de forma autónoma e individual.

c) El sistema para la actualización de contraseñas está diseñado para que las contraseñas sean mínimas de 8 caracteres, entre letras, números y caracteres especiales.

d) El sistema de gestión de contraseñas obliga al usuario a cambiar la contraseña cuando esta no haya cambiado en un periodo de seis meses.

9.4.4 Uso de programas utilitarios privilegiados

a) Se seguirán los lineamientos dados en el numeral 9.2.3 Gestión de Privilegios para prevenir el abuso de los mismos que ocasionen degradación o anulación de los controles del sistema.

b) El acceso a programas utilitarios en sistema está limitado por el controlador de dominio de acuerdo al tipo de usuario, donde se restringen la modificación de configuraciones del sistema, instalación de programas, entre otros relacionados.

c) El área de Tecnologías de la Información y Telecomunicaciones instalará o habilitará los programas en los sistemas en relación con lo requerido para cada usuario, en donde entregará el acta de entrega de equipo.

9.4.5 Control de acceso a código fuente de programas

a) Se deberá implementar mecanismos para la protección del código fuente de programas.

b) La lectura de código fuente de programas desarrollados internamente y externamente está prohibida, excepto para el área de Tecnologías de la Información y Telecomunicaciones.

10. CRIPTOGRAFÍA

10.1 CONTROLES CRIPTOGRÁFICOS

10.1.1Política sobre el uso de controles criptográfico

a) Los controles criptográficos tales como cifrado son aplicables a copias de seguridad, y equipos de usuarios portátiles que se determinen por razones de seguridad de la información.

El área de Tecnologías de la Información y Telecomunicaciones y seguridad de la Información está comprometida con la implementación de controles criptográficos, los cuales son necesarios para proteger la información que viaja a través del ciberespacio y cuando se guarda en medios de almacenamiento de las posibles amenazas que afectan los criterios de confidencialidad, integridad/autenticidad y no repudio.

b) Los activos expuestos por la entidad como servicios web, deben contar con un certificados SSL (Secure Sockets Layer) este protocolo criptográfico proporciona privacidad e integridad en la comunicación entre dos puntos en una red de comunicación; En el caso de correo electrónico se realiza a través del protocolo TLS (Seguridad en la capa de transporte) el cual proporciona la seguridad de cifrando en los correos para proteger su privacidad, adicional a esto el proveedor del servicio de correo electrónico brinda el servicio de almacenamiento cloud o almacenamiento de archivos en nube, en este tipo de cifrado todos los archivos que se suban o se creen documentos nuevos se encriptan en tránsito y en reposo.

Los certificados SSL para aplicaciones y TLS para el correo electrónico, investigan la existencia del sitio web, confirman su identidad y cifran la información que viaja por el ciberespacio.

c) Para el caso de los dispositivos de almacenamiento se realizan cifrados mediante diferentes mecanismos, según el tipo de información y datos.

d) En caso de requerirse con base a la importancia de información de usuarios se implementa el cifrado de equipos a través de herramientas de cifrado, esta actividad deberá ser llevada a cabo por el profesional de infraestructura TI y el Profesional Administrador SGSI, indicando el método de cifrado.

e) El profesional de TI es el encargado de adquirir o gestionar con los terceros el certificado SSL, para aplicarlos a las aplicaciones web, así como velar por la aplicabilidad del protocolo TLS en el correo electrónico y del empleo de mecanismos de cifrado en medios de almacenamiento externos.

Los usuarios podrán solicitar al área de Tecnologías de la Información y Telecomunicaciones la encriptación de los equipos de cómputo o medios asignados, esto a través de la herramienta de mesa de ayuda.

f) Toda aplicación desarrollada o adquirida por el CONSEJO PROFESIONAL debe contar con métodos y técnicas de criptográficos para el tratamiento de la información.

g) El CONSEJO PROFESIONAL al contar con métodos y técnicas criptográficas genera un impacto positivo al interior y exterior de la organización, ya que sus empleados internos

como colaboradores externos se sienten protegidos al saber que la información que viaja a través de las aplicaciones web, correo electrónico cuentan con un nivel de seguridad al igual que la información que reposa en medios de almacenamiento.

10.1.2 Gestión de llaves

a) Se mantendrá confidencialidad de las llaves de los controles criptográficos por el personal designado del área de Tecnologías de la Información y Telecomunicaciones, generalmente del Profesional de Infraestructura TI y el Profesional Administrador SGSI, y las partes relacionadas.

b) Las llaves criptográficas deberán ser entregadas bajo custodia. El CONSEJO PROFESIONAL, obtiene el certificado SSL a través de una entidad externa, para posteriormente aplicarlos a las aplicaciones web publicadas, en caso del correo electrónico es la entidad externa quien provee y gestiona el servicio relacionado con el protocolo de seguridad TLS.

c) Los usuarios consumidores de las aplicaciones web del CONSEJO PROFESIONAL, consultan cada aplicación utilizando el protocolo seguro de transferencia de hipertexto https, esto es debido a que el servidor contenedor de aplicaciones web de la entidad cuenta con el protocolo SSL instalado y configurado en el servidor, haciendo que la información que transita por el ciberespacio viaje segura y cifrada.

   Los usuarios del correo electrónico envían y reciben correos cifrados a través del protocolo TLS implementado por el proveedor de servicio.

d) La gestión de llaves criptográficas SSL correspondientes a aplicaciones desarrolladas por el CONSEJO PROFESIONAL, está a cargo del Ingeniero de TI, quien debe gestionar los certificados SSL en los casos de adquisición, renovación, eliminación o destrucción de los mismos.

   La gestión del protocolo de cifrado TLS como la implementación y demás acciones está a cargo de la entidad externa que provee el servicio, el Coordinador de TI debe velar por el cumplimiento de esta administración tercerizada.

e) Las llaves Los accesos a las herramientas de cifrado para la gestión de claves deben ser entregados bajo custodia. Si el CONSEJO PROFESIONAL requiere cambiar los certificados SSL para las aplicaciones Web, lo puede realizar eliminando el existente y adquiriendo uno nuevo con una entidad que provea este servicio.

f) Si las llaves y métodos criptográficos han resultado comprometidos a nivel de seguridad, estos deben ser cambiados inmediatamente en caso del certificado SSL se debe desinstalar el certificado comprometido y comprarse un certificado nuevo; Para el caso del correo electrónico y el protocolo TLS se debe comunicarse al proveedor del servicio y finalmente si se ven comprometidas las técnicas de cifrado en los dispositivos de almacenamiento, estas deben cambiar sus contraseñas de acceso.

g) Cuando un funcionario abandona la organización el área de Talento Humano informa al Área de Tecnologías de la Información y Telecomunicaciones para que esta retire los accesos correspondientes al funcionario.

h) En el caso de que una llave esté pérdida o dañada en cuanto a las aplicaciones web, el Profesional Administrador de Servidores puede solicitar y descargarla nuevamente por parte del vendedor del certificado SSL, en caso del servicio de correo electrónico se debe informar al proveedor para que realice los ajustes respectivos y finalmente en caso del almacenamiento de información en dispositivos externos, se debe solicitar al Coordinador de TI para que se le asigna nuevamente. Las llaves criptográficas de servidores y/o equipos de usuarios que se realizan a través de herramientas de cifrado serán gestionadas (generadas, recuperadas, desactivadas, etc.) por las mismas herramientas.

i) Los respaldos de llaves y procedimientos criptográficos SSL y custodia de claves de acceso, está a cargo del Coordinador de TI en la organización.

11. SEGURIDAD FISICA Y DEL ENTORNO

11.1 ÁREAS SEGURAS

11.1.1 Perímetro de seguridad física

En la sede se tendrán puertas con controles de acceso para proteger las áreas que contienen información y servicios de procesamiento de información, como son los candados y las cerraduras en las puertas para el acceso dentro de la edificación y áreas.

Todos los funcionarios del CONSEJO PROFESIONAL deberán acceder a las instalaciones del CONSEJO PROFESIONAL y registrar su huella en el lector biométrico en la sede que tengan este control.

El personal de las recepciones deberá permitir el ingreso a los funcionarios que ya se encuentren vinculados laboralmente con la entidad y a los visitantes o partes interesadas con su respetivo proceso de ingreso.

Los funcionarios deben permanecer identificados con sus tarjetas o carnets corporativos, estos son de carácter personal e intransferible; la pérdida o hurto de los carnets y de identificación deben ser notificadas inmediatamente al área de Tecnologías de la Información y Telecomunicaciones.

Todas las áreas de la infraestructura física en la sede del CONSEJO PROFESIONAL son monitoreadas por circuito cerrado de televisión, ubicado en el centro de cómputo o datacenter.

Existen áreas donde los usuarios pueden acceder sin un control determinado, esta área es identificada como de atención al usuario, áreas de carga o baños públicos en donde los usuarios del CONSEJO PROFESIONAL realizan sus gestiones y trámites correspondientes en este caso el nivel de acceso es público.

Por otro lado, existen áreas o zonas comunes dentro de la infraestructura del CONSEJO PROFESIONAL como son las salas de espera, recepciones, pasillos, baños, auditorios, entre otros, donde el ingreso a estas áreas está determinado para los empleados y visitantes previamente identificados y registrados.

Finalmente existen áreas o zonas restringidas dentro de la entidad las cuales requieren un nivel de acceso de funcionarios con privilegios los cuales para el acceso requiere identificación, autorización y anuncio de ingreso, estas áreas restringidas son las oficinas de presidencia / Secretaria Ejecutiva, datacenter, circuito cerrado de cámaras de seguridad y archivo físico y material.

Existe un área de recepción en donde los visitantes deben ser anunciados sin excepción a los funcionarios con los cuales desean contactarse, a través de mensajería instantánea o por teléfono.

Dentro del edificio no es permitido el ingreso de funcionarios o visitantes con objetos emisores de ruidos permanentes molestos evitando así la contaminación auditiva.

En caso de alarmas contra incendios dentro del edificio, desde el área de recepción se desbloquea las puertas de acceso del edificio con el fin de que los empleados y visitantes puedan evacuar lo más pronto posible.

Para determinar accesos no autorizados o intrusos, el personal de EL CONSEJO PROFESIONAL debe portar el respectivo carnet de la entidad el cual contiene la fotografía del funcionario, nombre, área a la que pertenece entre otros datos que lo identifican como un empleado.

11.1.2 Controles de acceso físico

El personal de las recepciones podrá permitir el ingreso a los visitantes que han sido previamente autorizados por un funcionario de la entidad.

Los funcionarios deberán recoger al visitante en la recepción de la entidad para indicarle el espacio en donde se desarrollará la visita, momento a partir del cual el funcionario se hace responsable del visitante.

En los casos en que se presenten daños, robos o cualquier tipo de inconvenientes con visitantes que no hayan cumplido con los requisitos expuestos anteriormente será responsabilidad del funcionario que autorizó el ingreso, o del personal de recepción en caso de que ningún funcionario haya autorizado el ingreso del visitante.

a) El ingreso de visitantes o terceros a la entidad solo se podrá realizar en horario hábil de lunes a viernes de 8 a.m. a 3:30 p.m. Los ingresos en horarios adicionales deben ser solicitados con antelación por escrito (correo electrónico u oficio) a Talento Humano.

b) El ingreso de visitantes a las áreas donde se procesa información como el centro de datos datacenter no está autorizado, en caso de requerir el acceso debe estar acompañado del personal autorizado; si se requieren realizar actividades de mantenimiento en el datacenter

por parte de proveedores debe hacerse bajo el acompañamiento y supervisión de personal interno de la entidad, para el caso de acceso al data center se debe diligenciar el documento tipo formato control de acceso al datacenter, en donde queda registrado los datos de ingreso del visitante proveedor, fecha y hora de ingreso, empleado responsable de la visita, y la justificación del acceso entre otros datos de registro

c) Los proveedores de Servicios de Internet como ISP u otros servicios relacionados con el centro de cómputo y que requieran acceso físico están restringidos y solo se les autoriza el ingreso junto con el personal interno autorizado por la entidad y el registro en el formato control de acceso al datacenter.

d) El CONSEJO PROFESIONAL revisa constantemente los controles de acceso a áreas restringidas asignando o retirando controles en los casos donde los funcionarios ya no pertenezcan a la entidad o cambien de cargo.

11.1.3 Seguridad de oficinas, recintos e instalaciones

a) El ingreso de funcionarios está permitido en el horario hábil establecido para cada sede, en otros horarios se debe solicitar previamente con el visto bueno del secretario(a) o director respectivo.

El ingreso del personal público o visitantes a los centros de generación de información en el CONSEJO PROFESIONAL como data center deben estar restringidos físicamente con candados y cerradura de apertura de puerta.

b) El ingreso de visitantes o terceros a la entidad solo se podrá realizar en horario hábil de lunes a viernes de 7am a 11am y de 1pm a 4pm. Los ingresos en horarios adicionales deben ser solicitados con antelación por escrito (correo electrónico u oficio) a Talento Humano

c) Los visitantes deben ser anunciados sin excepción por el personal de recepción a los funcionarios con los cuales desean contactarse, a través de mensajería instantánea o por teléfono. El personal de recepción debe verificar visualmente si el visitante lleva algún equipo, así como las características de identificación del equipo y realizar el registro al ingreso y salida.

d) Los funcionarios deberán recoger al visitante en la recepción para indicarle el espacio en donde se desarrollará la visita, momento a partir del cual el funcionario se hace responsable del visitante.

En los casos en que se presenten daños, robos o cualquier tipo de inconvenientes con visitantes que no hayan cumplido con los requisitos expuestos anteriormente será responsabilidad del funcionario que autorizó el ingreso, o del personal de recepción en caso de que ningún funcionario haya autorizado el ingreso del visitante.

En las recepciones de la entidad no deberá existir listado de números telefónicos y direcciones físicas de oficinas visibles al público.

11.1.4 Protección contra amenazas externas y ambientales

a) El CONSEJO PROFESIONAL contará en las oficinas y áreas convenientes con elementos de atención de emergencias como extintores y botiquines; el área de Talento Humano velará por su consecución y por el buen estado de los mismos.

11.1.5 Trabajo en áreas seguras

a) Se entienden como zonas restringidas o áreas seguras las siguientes:

- Archivo Central
- Centros de Cómputo
  Los accesos a las zonas de datacenter están dados para los siguientes cargos
- Coordinador TIC
- Técnico de Tecnología (Redes y Telecomunicaciones)
- Personas de Seguridad Informática.

Toda persona adicional que requiera ingresar debe registrarse indicando fecha, hora entrada, nombre, firma, hora de salida, firma del funcionario que autoriza y motivo del ingreso.

b) Las zonas restringidas deben estar debidamente identificadas, contar con mecanismos de control de acceso, y monitoreo mediante CCTV (Circuito Cerrado de Televisión), solo los funcionarios del proceso están autorizados a ingresar a estas zonas. Si un funcionario de otra área requiere ingresar, puede hacerlo bajo autorización y responsabilidad del coordinador del área; Están autorizados a ingresar al centro de cómputo.

c) Las áreas vacías de la organización, como depósitos de almacenamiento, están monitoreadas con sistemas de CCTV (circuito cerrado de televisión) con el fin de identificar accesos indebidos por parte de empleados o visitantes.

d) Está prohibida la toma de fotografías en los Centros de Cómputo sin autorización de la Coordinación de TI o presidencia / Secretaria Ejecutiva.

11.1.6 Áreas Públicas Áreas de Despacho y Carga

a) El CONSEJO PROFESIONAL cuenta con un el público en general solo puede ingresar a las áreas públicas en los horarios establecidos para el público.

El CONSEJO PROFESIONAL cuenta con dos zonas de despacho y carga una destinada al envío y recepción de paquetes y correspondencia de un tamaño y peso menor la cual se encuentra en el primer piso de la entidad, y otra zona ubicada en el sótano del edificio destinado para correspondencia de mayor peso y tamaño; El personal visitante que accede

al área de despacho y carga de EL CONSEJO PROFESIONAL, debe estar debidamente identificado.

b) Se consideran áreas públicas las Recepciones, áreas de despacho y carga, vestíbulos de ascensores y zonas de atención al público.

El personal de despacho y carga visitante tiene acceso únicamente a las áreas definidas para este fin, en donde se cargan y descargan insumos o correspondencia para el funcionamiento de la entidad.

c) No se permite acceso de personal armado a las oficinas.

Durante el proceso de carga y descarga el personal empleado del CONSEJO PROFESIONAL deberá asegurar las puertas de acceso internas a las zonas de despacho y carga evitando accesos no autorizados a la entidad.

d) La correspondencia deberá ser entregada en la recepción de las oficinas en el horario establecido para ellos. Si se requiere la entrega de correspondencia personalmente a un funcionario, éste deberá ir a recibirla a la recepción.

En todos los casos la correspondencia es inspeccionada por los empleados de la entidad para este caso el auxiliar administrativo, el cual reportará la existencia de posibles anomalías en paquetes defectuosos, sospechosos de explosivos, químicos inflamables u otros materiales peligrosos, en caso de detectar este tipo de correspondencia, se procede a informar.

e) Los activos de información que ingresen por las zonas de despacho y carga deben ser registrados y asignados a un empleado por el área de Talento Humano.

f) La correspondencia entrante y saliente están debidamente separadas y arrumadas en pilas para su identificación.

11.2 SEGURIDAD DE LOS EQUIPOS

11.2.1 Ubicación y protección de los equipos

a) Los equipos portátiles no deberán estar ubicados en áreas públicas, en los casos en los que se requiera deberán estar asegurados con guaya.

b) Los equipos de generación de información, estarán protegidos por medio de los controles de acceso físico, así como por otros mecanismos como guayas de seguridad si se requiere, que serán implementados por el área Administrativa.

c) Los accesos a las instalaciones físicas en donde se almacenan los equipos de cómputo, están restringidos para los funcionarios externos.

d) Al llegar algunos equipos de cómputo críticos a las zonas de descarga, estos no deberán permanecer demasiado tiempo sin ser entregados.
e) En las áreas de almacenamiento de equipos de cómputo deben estar libres de amenazas físicas como, electromagnetismo, humedad, robo, incendio entre otras.

f) Los empleados de la organización No deben consumir alimentos en sus puestos de trabajo sobre los equipos de cómputo.

11.2.2 Servicios de suministro

a) Los servicios de suministros de electricidad para los equipos y servidores están bajo la responsabilidad del área de gestión de ti apoyados en el área de talento Humano.

b) Los servicios de suministros de electricidad para los equipos y servidores críticos se tendrá soporte de UPS para el caso en que haya una falla en el suministro eléctrico.

c) Los servicios de suministros de telecomunicaciones están bajo la responsabilidad del proceso de Gestión de TI

d) Los servicios de suministros tales como redes de agua, gas, ventilación y relacionados estarán bajo la responsabilidad del área Administrativa.

11.2.3 Seguridad del cableado

a) El cableado de energía eléctrica y de telecomunicaciones debe ir por ductos o canaletas que impidan daño accidental al mismo.

b) El cableado estructurado de datos debe ser independiente o con medidas de aislamiento del cableado eléctrico.

c) Se debe realizar mantenimiento a los centros de cómputo y centros de cableado al menos una vez al año y cargar los registros en la plataforma definida.

11.2.4 Mantenimiento de los equipos

a) Se debe entregar el plan de mantenimientos para el año que inicia a más tardar el 31 de enero de cada año.

b) Se realizará mantenimiento a los equipos de los funcionarios una vez al año.

c) El mantenimiento de los servidores se debe realizar una vez al año acompañado de un proceso documentado de gestión de cambios. Los registros de estos mantenimientos se deben cargar en la plataforma definida.

d) Al realizar mantenimientos o actividades que impliquen modificación de configuraciones se debe tomar Backups de las configuraciones al iniciar la actividad, y nuevamente

Backups después de guardar todos los cambios y finalizar la actividad y almacenarlos en un repositorio compartido por el área de Tecnologías de la Información y Telecomunicaciones.

11.2.5 Retiro de activos

a) El ingreso de equipos externos, y la salida de equipos corporativos debe estar autorizado por el secretario o Coordinador de TI llenando el formato Solicitud de Préstamo y Retiro de Equipos.

b) En cada área la información bajo su custodia no debe ser retirada sin la autorización del coordinador o director a través de ningún medio.

11.2.6 Seguridad de equipos y activos fuera de las instalaciones

a) Se debe prestar especial atención a los dispositivos, tales como: computadores portátiles, tablets, discos duros externos, tabletas, teléfonos inteligentes, memorias USB y en general todo dispositivo que contenga información del CONSEJO PROFESIONAL, con los siguientes controles: Tecnologías de cifrado para la información confidencial residente en el disco duro cuando sea necesario y contraseña fuerte de inicio de sesión.

b) Utilizar todas las recomendaciones definidas en la política de seguridad sobre contraseñas.

c) No usar en redes públicas inalámbricas los dispositivos del CONSEJO PROFESIONAL que contengan información confidencial.

d) Evitar exponer el equipo a factores externos que comprometan su integridad, tales como, calor extremo, humedad, electromagnetismo, radiación, humo o polución.

e) Los equipos sólo deben ser conectados a redes que tengan corriente regulada.

f) Llevar el portátil como equipaje de mano en viajes.

g) No se deben acceder a los servicios de TI del CONSEJO PROFESIONAL MVZ como el Correo, VPN y demás servicios corporativos desde redes de datos sitios que no sean de confianza, tales como Wifi público, cafés internet y relacionados.

h) Los equipos e información no se deben dejar desatendidos o sin vigilancia en lugares públicos.

11.2.7 Disposición segura o reutilización de equipos

El área de Tecnologías de la Información y Telecomunicaciones debe realizar formateo de bajo nivel al disco duro de todos los equipos que se reciban por devolución de activos, ya sea para reasignar el equipo a otro funcionario, para devolverlo al proveedor del alquiler, o para darlo de baja.

11.2.8 Equipos de usuario desatendido

a) Es obligatorio el realizar el bloqueo de pantalla (Tecla Windows + L) de la estación de trabajo o computador por parte del funcionario cada vez que éste abandone su puesto de trabajo para evitar accesos no autorizados a su información.

b) Se contemplarán dentro las configuraciones de los sistemas un posible control de los tiempos de conexión e inactividad, el cual puede variar entre los diversos sistemas de información según las consideraciones de buenas prácticas de TI analizadas por el área de Tecnologías de la Información y Telecomunicaciones.

11.2.9 Política de escritorio despejado y de pantalla despejada

a) Los archivadores y cajones de escritorios que contengan información confidencial deben estar cerrados con llave.

b) No dejar documentos confidenciales a la vista de otras personas ya sea en el puesto de trabajo o en el escritorio del computador.

c) No arrojar documentos confidenciales a la basura, estos deben ser destruidos.

d) Al finalizar las labores diarias o si el funcionario se va a ausentar de su puesto de trabajo, todos los documentos confidenciales deben ser guardados en sitio seguro.

e) Los papeles autoadhesivos que contengan información confidencial, especialmente contraseñas están prohibidas.

f) Está prohibido escribir las contraseñas de los funcionarios en papeles, debajo del teclado, en cajoneras o sobre el escritorio.

g) Los trabajos de impresión que contengan información confidencial deben ser recogidos de forma inmediata por quien los origina.

h) La impresión de documentos como .PDF confidenciales debe estar bloqueada o protegido con clave.

12. SEGURIDAD DE LAS OPERACIONES

12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

12.1.1 Procedimientos de operaciones documentados

a) Los instructivos y manuales que por contener datos restringidos que solo conciernen al área de Tecnologías de la Información y Telecomunicaciones no será conveniente que se carguen en el sistema de Gestión Documental, estarán disponibles en el área de TI.

b) Los procedimientos del área de Tecnologías de la Información y Telecomunicaciones se revisarán al menos una vez al año y se actualizarán cuando sea necesario.

12.1.2 Gestión de cambios

a) Cualquier cambio a la plataforma tecnológica del CONSEJO PROFESIONAL deberá ser completamente documentado y controlado a través de un proceso de gestión de cambios en la herramienta de mesa de ayuda. Se deben detallar las actividades previas, las actividades durante el cambio, las actividades posteriores al cambio y las actividades en caso de regreso del cambio.

b) Los Propietarios de la información, Administradores de los sistemas o Ingenieros de producto que originan el cambio, son los responsables de presentar el cambio y coordinar todas las actividades para su ejecución.

c) Los cambios que se lleven a cabo deben ser evaluados y probados de forma integral y se debe contar con una participación de los administradores de los diferentes componentes de la solución.

d) En el proceso de gestión cambios se deben considerar los niveles de servicio y las necesidades de la organización.

e) En el proceso de gestión cambios se debe incluir la identificación de los riesgos asociados al cambio y las acciones del tratamiento correspondiente.

f) Todos los mantenimientos y/o cambios deben tener visto bueno de:

- Coordinador de TIC

g) La validación del funcionamiento de los sistemas posterior al cambio debe incluir al menos a un coordinador de los procesos que usan los sistemas implicados en el cambio.

12.1.3 Gestión de capacidad

Se realizará seguimiento al uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.

a) El Proceso de Infraestructura TI gestiona las capacidades de los equipos de cómputo, servidores y dispositivos activos de interconexión, que contengan información no requerida u obsoleta dentro por la organización, esta debe quedar disponible y alojada en modo de solo lectura, evitando que sea modificada y que tenga un incremento de espacio. En los mantenimientos de estaciones de cómputo se eliminan archivos temporales liberando espacio en disco duro.

b) Las bases de datos y aplicaciones obsoletas, son excluidas de las rutinas de Backups ahorrando espacio y procesamiento en la generación de las mismas, se deja una copia de seguridad única en caso de que el sistema falle.

c) Los procesos de generación de información que requieran grandes bloques de datos, son analizados en motores de bases de datos diferentes a los de producción.

d) El código de las aplicaciones es optimizado por el proceso de desarrollo junto con el DBA.

e) El consumo de navegación es controlado por el firewall de nueva generación, mitigando el consumo indiscriminado de ancho de banda e internet.

12.1.4 Separación de los entornos de desarrollo, pruebas y producción

a) En los desarrollos de aplicaciones internas tendrá separados en entornos de desarrollo, pruebas o preproducción y producción para los aplicativos; Para los aplicativos desarrollados externamente se tendrá únicamente el entorno de producción en el CONSEJO PROFESIONAL, el entorno de desarrollo será responsabilidad del proveedor, y el entorno de pruebas se definirá de común acuerdo entre las partes cuando haya lugar a un cambio. Este será documentado mediante un proceso de gestión de cambios.

b) Los ambientes de desarrollo, pruebas y producción funcionan independientes del tipo de tecnología Hardware, lo que las hace portables en cuanto a infraestructura.

c) Los desarrollos de aplicaciones internas y externas son evaluados en un ambiente de pruebas o preproducción, el cual tiene las mismas características de un ambiente de producción, con el fin de evaluar las funcionalidades de los desarrollos.

d) No se deben realizar pruebas o validación de códigos en los ambientes de producción de aplicaciones y bases de datos, todo desarrollo debe validarse en pruebas.

e) El acceso a aplicaciones y bases de datos de producción estará autorizado por el Coordinador de TI.

f) El acceso a las bases de datos de los ambientes de producción, cuenta con roles para los usuarios de solo consulta.

g) La información transaccional de las operaciones en aplicaciones productivas no debe apuntar a bases de datos de pruebas, debe ser a las bases de datos de producción.

12.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

12.2.1 Controles contra códigos maliciosos

a) Todos los equipos de funcionarios y terceras partes que se conecten a la red cableada o inalámbrica de la entidad deben tener instalado antivirus. Los usuarios son responsables

de que el antivirus de su equipo esté instalado, habilitado y actualizado, y de que se haya realizado al menos un escaneo la última semana.

Los funcionarios no deben instalar programas o aplicaciones no autorizadas sin la debida autorización por parte del área de Tecnologías de la Información y Telecomunicaciones.

b) Los funcionarios no deben instalar ni utilizar en equipos del CONSEJO PROFESIONAL (propios o alquilados) software sin la debida autorización del área de Tecnologías de la Información y Telecomunicaciones. El personal de Tecnología puede instalar software para pruebas, evaluación y para cumplir sus funciones con las debidas precauciones y bajo su responsabilidad.

c) Es responsabilidad de cada funcionario o tercero, revisar que todos los medios extraíbles sean chequeados con un antivirus antes de procesarlos en los computadores personales o servidores el CONSEJO PROFESIONAL.

Si se detectan sitios web peligrosos que representen una amenaza o que contengan códigos maliciosos, el proceso de seguridad de la información debe bloquear aquellos inmediatamente.

d) Es responsabilidad del área de Tecnologías de la Información y Telecomunicaciones mantener en cuanto a configuración, actualización y licenciamiento las herramientas y procedimientos que permitan prevenir, detectar y corregir incidentes por código malicioso.

Los funcionarios deben realizar la validación de la información intercambiada con entidades externas, en caso de no poder hacerlo debe solicitar ayuda al proceso de Seguridad de la Información

e) Es responsabilidad del área de Tecnologías de la Información y Telecomunicaciones distribuir las actualizaciones del sistema operativo a los equipos del dominio reduciendo las vulnerabilidades.

f) El antivirus debe ser administrado desde una consola central para que periódicamente realice las actualizaciones de firmas, escaneo de detección de código malicioso y reporte centralizado.

g) Los equipos que reporten código malicioso o virus serán aislados de la red LAN hasta tanto sea remediado y se implementen los controles de protección.

h) En caso de ser víctima de un malware se debe contar con mecanismos que garanticen la continuidad de la entidad, garantizando el restablecimiento de las operaciones en un tiempo acordado, como por ejemplo copias de respaldo de la información.

i) Los correos electrónicos que provengan vengan de personas desconocidas deben ser tratados con precaución. No se deben abrir los archivos anexos a los correos electrónicos,

cuyo origen es desconocido o el mensaje no tiene una relación con las actividades del CONSEJO PROFESIONAL.

12.3. COPIAS DE RESPALDO

12.3.1 Respaldo de la información

a) Se realizarán copias de seguridad de la información almacenada en las bases de datos y aplicativos seleccionados. Las copias de seguridad a los usuarios sólo se realizarán a la información almacenada en la unidad compartida.

b) Se realizará copia de los Backups de información crítica, del CONSEJO PROFESIONAL serán programados.

c) Para todos los aplicativos de los cuales se haga respaldo de información se verificará una vez al mes un Backups aleatorio con el fin de verificar que la información se pueda restaurar correctamente, igualmente cuando se modifique el método de generación del Backups. Será responsabilidad del Profesional de TI (Backups y bases de datos) y en la sede de Contingencia del Profesional de Tecnología Departamental de la misma; En el caso de las restauraciones de las bases de datos la responsabilidad es compartida entre el Coordinador de TI y el Auxiliar o técnico de sistemas; cualquier falla en el proceso de restauración será reportada de inmediato al proceso de Seguridad de la Información.

d) Los empleados el CONSEJO PROFESIONAL, pueden solicitar al proceso de Administración de Infraestructura Tecnológica la generación del Backups de su equipo de cómputo mediante correo electrónico.

e) Los empleados del CONSEJO PROFESIONAL están en la obligación de permitir realizar las copias de seguridad de los equipos de cómputo asignados en el momento que el área de Tecnologías de la Información y Telecomunicaciones así lo requiera.

12.4 REGISTRO Y SEGUIMIENTO

12.4.1 Registro de eventos

a) El proceso de Administración de Infraestructura Tecnológica a través de los sistemas, aplicativos y herramientas tecnológicas realizará monitoreo de los registros de eventos de las actividades de usuarios, excepciones, fallas y eventos de seguridad de la información.

b) En el registro de eventos de usuarios se contemplarán datos que permitan la identificación de usuarios y relacionados a las actividades de los sistemas, datos cronológicos, fechas y horas, detalles de eventos de ingresos, salidas, conexiones o desconexiones, manipulación de documentos, archivos, herramientas, programas, detalles de direccionamiento y protocolos de red, registro de transacciones entre otros relacionados a las actividades de los usuarios.

c) El proceso de Administración de Infraestructura Tecnológica y el de Seguridad de la Información en el registro de eventos deberá contemplar y cumplir todos los mecanismos para preservar la confidencialidad, integridad y disponibilidad de la información, así como la protección de datos personales y datos sensibles de los usuarios.

d) Los datos e información obtenida de los eventos serán utilizados exclusivamente para los fines de investigaciones en la prevención de incidentes de seguridad en protección del sistema de información y la salvaguarda de los datos corporativos.

12.4.2 Protección de la información de registro

a) El proceso de Infraestructura Tecnológica debe realizar las configuraciones pertinentes para la protección de la información de registros o log generados por el sistema de información y sus componentes, de tal manera que se pueda preservar la confidencialidad, integridad y disponibilidad.

b) Los Logs serán almacenados y custodiados en un medio de almacenamiento externo en caso de necesitar liberar espacio del servidor, estará dividido por períodos determinados y variaran según el componente del sistema de información, tales como servidores de aplicación, web cervices, servidores de bases de datos, terminales brutas, entre otros.

c) El acceso a los Logs o información de registros es permitido al personal del proceso de Infraestructura Tecnológica quienes son administradores del Data Center y podrán ser entregados a otros procesos a las coordinaciones o direcciones por medio de solicitud formal justificada y donde se expongan para que fines requeridos se necesitan.

12.4.3 Registros del administrador y del operador

El proceso de Infraestructura Tecnológica debe proteger y revisar periódicamente los registros o Logs de los administradores y operadores de componentes del sistema de información, tales como servidores de aplicación, web services, servidores de bases de datos, terminales brutas, entre otros.

Se debe velar por la protección de los Logs en cuestión, la modificación o alteración de dichos logs por parte de los administradores u operadores se considera una falta grave en contra de la seguridad de la información y dichas actividades serán evidenciadas y reportadas a talento humano y jurídica para que se proceda con el proceso disciplinario.

12.4.4 Sincronización de relojes

a) Los sistemas de información corporativos se sincronizan contra el servidor de dominio de aplicaciones principales.

b) La sincronización de relojes de equipos de municipios o nodos con conexión banda ancha se sincronizará automáticamente y la zona horaria será UTC-05:00 Bogotá.

12.5 CONTROL DE SOFTWARE OPERACIONAL

12.5.1 Instalación de Software en Sistemas Operativos

a) La instalación de software en los computadores suministrados por el CONSEJO PROFESIONAL y de los equipos conectados a la red corporativa es una función exclusiva del área de Tecnologías de la Información y Telecomunicaciones. Toda instalación debe tramitarse a través de una solicitud del área de Tecnologías de la Información y Telecomunicaciones, quien removerá sin previo aviso los archivos que claramente incumplan con las normas señaladas en esta política.

b) Todo software o contenido multimedia utilizado en los equipos propiedad de la compañía, de los equipos conectados a la red corporativa o que se utilicen en las instalaciones del CONSEJO PROFESIONAL deben poseer las licencias de uso legal, de acuerdo a leyes de protección de propiedad intelectual y derechos de autor.

c) El área de Tecnologías de la Información y Telecomunicaciones mantendrá listas actualizadas del software estándar autorizado para instalar en los computadores, de acuerdo a cada área o grupo. Tecnologías de Información y Telecomunicaciones solo instalará software estándar de acuerdo a la disponibilidad de licencias de uso.

d) Para requerimientos de software no estándar, la solicitud debe ser realizada por el coordinador del funcionario al área de Tecnologías de la Información y Telecomunicaciones, quien debe realizar una evaluación de las vulnerabilidades de seguridad y licencias del software y solo si hay un concepto favorable se procederá a realizar la instalación del mismo.

e) En el caso de actualizaciones de software que afecten el correcto funcionamiento del sistema, se debe realizar un rollback volviendo a la versión anterior, por ejemplo, en el caso de los controladores.

12.6 GESTIÓN DE LA VULNERABILIDAD TÉCNICA

12.6.1 Gestión de la vulnerabilidad técnica

Se realizará análisis de vulnerabilidades de los activos críticos principalmente a los de la data center de forma periódica al menos una vez al año.

a) El proceso de seguridad de la información y protección de datos, debe realizar el análisis de vulnerabilidades en los activos de mayor importancia y que afectan la correcta operación de la organización.

b) El proceso de seguridad de la información analiza las vulnerabilidades e informará vía correo electrónico generando un registro en la plataforma de mesa de servicio al área

encargada sobre las posibles medidas correctivas esto puede incluir actualizaciones o aplicación de parches de seguridad.

c) Una vez entregados los resultados y correcciones de las vulnerabilidades, el proceso de seguridad de la información y protección de datos dará un tiempo prudente para que el área correspondiente realice las correcciones sugeridas.

d) Si la corrección de las vulnerabilidades implica instalaciones de parches o configuraciones de gran impacto, se deben realizar las validaciones funcionales en ambientes de pruebas antes de hacerlo directamente en los servidores de producción.

e) Una vez terminado este tiempo para la implementación de las correcciones, se volverá a ejecutar el análisis de vulnerabilidades.

f) Si la corrección de la vulnerabilidad no es posible ejecutarla, se debe asumir el riesgo por parte de los actores y áreas involucradas, se implementarán medidas para mitigar el riesgo como por ejemplo la generación de copias de seguridad con más frecuencia entre otras medidas.

12.6.2 Restricciones sobre la instalación de software

a) Las instalaciones de software en los equipos de cómputo están controladas a través de las políticas del servidor de dominio principal para las estaciones de cómputo.

b) Los usuarios que por la naturaleza de sus funciones requieran tener privilegios para la instalación de software se les podrá agregar a grupos especiales y controlados en el servidor de dominio para levantar las restricciones pertinentes.

c) Por defecto los usuarios no pueden realizar instalaciones en los equipos de cómputo, ni ellos deberán hacerlos, en caso de requerirse algún tipo de Software deberá realizarse las solicitudes al área de Tecnologías de la Información y Telecomunicaciones a través de los canales ya definidos para que evalúen las vulnerabilidades de la aplicación solicitada.

d) También se deben seguir las directrices definidas en la política del numeral 12.5.1 *Instalación de Software en Sistemas Operativos*.

12.7. CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN

12.7.1 Controles sobre auditorias de sistemas de información

a) El área de Control Interno deberá llevar a cabo las auditorías internas y realizará acompañamiento de las auditorías externas que se realicen a los sistemas de información con el fin de llevar los controles respectivos de cumplimiento.

b) El área de Control Interno es el responsable de velar por el cumplimiento de las políticas establecidas por los entes reguladores y las políticas internas y verificar que la organización cumpla con lo que está establecido en los procedimientos, manuales, formatos, instructivos y procesos establecidos por el SGSI. Realizará auditorías periódicamente incluyendo en su alcance el SGSI y si encuentra no conformidades verificará que se establezca un plan de mejora con tareas, responsables y fechas de cumplimiento definidas. Asimismo, verificará que la tarea realmente le apunte a la mejora, que la solución planteada sea coherente con la causa de la no conformidad y que se ejecute en el tiempo establecido en el plan de mejora.

c) El proceso de Infraestructura TI, debe tener habilitadas las auditorías en las bases de datos más críticas de la organización, en el caso de que sean requeridas por procesos como Control Interno.

13. GESTIÓN DE LA SEGURIDAD DE LAS COMUNICACIONES.

13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES.

13.1.1 Controles de las redes

a) Se revisarán dentro de los análisis de riesgos de seguridad de la información los puntos únicos de falla en las redes para mitigar que se produzcan eventos de indisponibilidad de las mismas.

Las redes en el CONSEJO PROFESIONAL son administradas por el área de Tecnologías de la Información y Telecomunicaciones.

b) Se controlará el acceso a las redes mediante VLANs e inhabilitación de puntos de red no utilizados.

c) Las actividades relacionadas con la administración de redes, solo aplican a dispositivos activos de interconexión como switches, rourter y firewalls propietarios.

En el caso de dispositivos de interconexión no propietarios entregados por proveedores a la entidad, el Profesional Administrador de Redes y Telecomunicaciones solicita acceso con roles definidos para poder realizar esta administración, en caso de no poder hacer cambios a través de estos roles por carencia de privilegios, estos deben hacerse directamente por el proveedor del servicio.

d) Los accesos y la seguridad en las redes inalámbricas están determinados por el protocolo WAP2 (Acceso Wi-Fi protegido 2) basado en el estándar 802.11 N/ac el cual utiliza el método de cifrado AES (Advanced Encryption Standard). Además, para tener el servicio se debe ingresar la dirección MAC del equipo de cómputo cliente en el dispositivo de Interconexión.

e) Todos los equipos de cómputo asociados a los dispositivos activos de interconexión inalámbrica son clasificados en roles preestablecidos en los dispositivos de interconexión donde son segmentados en la red.

13.1.2 Seguridad de los servicios de la red.

a) Los servicios publicados hacia Internet que requieran usuario y contraseña para acceder a información confidencial estarán protegidos mediante técnicas de cifrado SSL, TLS, AES o similares, y algunas tecnologías de red como VPN, las cuales están descritas en esta política en el punto 10.1.1. numeral b.

El grupo de funcionarios de TI, es el encargado de gestionar las conexiones y capacidades de los canales en las redes de comunicación internos y externos, así como la administración y cambios en los dispositivos activos de interconexión de red.

b) Los acuerdos de nivel de servicio que se establezcan para los servicios de red tendrán en cuenta los requerimientos de seguridad, los niveles de servicio, los puntos de contacto y los procedimientos a ejecutar en caso de fallas. El CONSEJO PROFESIONAL, cuenta con una red de telecomunicaciones definida, como estructurada y segmentada, para poder acceder a esta red mediante VPN, los usuarios deben cumplir con criterios de seguridad y de conexión como contar con una conexión de red estable la cual consume entre un 30% y un 60% de la conexión a Internet, dependiendo de la proximidad al servidor VPN; Adicional a esto las credenciales de accesos deben ser certificados por parte de la compañía.

c) El proceso de Seguridad de la Información y Protección de Datos es el encargado de permitir o denegar los servicios de red implementados por el proceso de Infraestructura TI en el firewall perimetral, basado en criterios de afectación que involucren la confidencialidad, integridad y disponibilidad de la información.

13.1.3 Separación en las redes

a) Se tendrán separadas por medio métodos de segmentación de redes LAN virtuales (VLANs) los servidores de los equipos de usuario.

b) Los servidores publicados hacia Internet serán accedidos a través de una zona DMZ con acceso controlado a la LAN.

c) Los servidores no deben tener salida a Internet, excepto el Antivirus y WSUS para descarga de actualizaciones.

d) La separación de redes está dada por los diversos componentes de red, y se controlan principalmente por UTM y/o Firewalls.

e) Las redes inalámbricas están en una red más restrictiva en una VLAN independiente y aislada lógicamente del resto de la LAN.

13.2 TRANSFERENCIA DE INFORMACIÓN

13.2.1 Políticas y procedimientos para la transferencia de información

a) La transferencia de información entre el CONSEJO PROFESIONAL y sus prestadores de servicios de salud, contratistas, proveedores y otros terceros debe realizarse cumpliendo con las condiciones y lineamientos descritos a lo largo de este documento.

La entrega y recepción de información con entidades externas, se realiza empleando dispositivos de almacenamiento, correo electrónico, unidades compartidas con almacenamiento cloud y consumo de web services.

Se debe validar los ssl para web services internos y externos

b) Para la entrega de información digital en unidades de almacenamiento a entes de control y como parte de requerimientos judiciales, esta debe ser entregada por el Coordinador de Tecnologías de la Información y Telecomunicaciones mediante acta indicando el tamaño total de la información y el Hash SHA-256 de la misma. El Profesional Administrador SGSI debe verificar que la información entregada corresponda a lo detallado en el acta.

c) La información transferida que llega en formatos adjuntos por vía correo electrónico y que es categorizada dentro del mismo como spam o correo altamente peligroso, debe ser comunicada al proceso de seguridad de la información y Protección de Datos.

d) El correcto uso de los activos de información, está descrito en esta política de seguridad en el uso aceptable de los activos de información en el punto 8.1.3. de esta política.

e) Los funcionarios del CONSEJO PROFESIONAL, en su oficio de transferencia de entrega de información deben garantizar la calidad de la misma en términos de lectura, el proceso de Infraestructura TI es quien provee el medio de almacenamiento para la transmisión solicitado por las entidades externas, y finalmente el proceso de Seguridad de la Información y Protección de Datos resguarda el medio en que se entrega la Información.

Los funcionarios del CONSEJO PROFESIONAL, en su oficio de recepción de información por entidades externas deben reportar las inconsistencias encontradas en la información recibida tanto a la entidad externa como al proceso de Seguridad de la Información.

f) La forma como está protegida la información transferida está soportada en métodos de acceso y criptográficos definidos en el punto 10 de esta política.

g) Toda la Información transferida y recibida mediante dispositivos de almacenamiento de entidades externas debe tener una copia de respaldo realizada por el área de Infraestructura TI y esta debe permanecer en custodia.

Cuando se transfiera información por correo electrónico, se debe guardar el correo electrónico como evidencia de recepción o envío de la información.

Cuando se transfiera información utilizando almacenamiento en cloud para ser compartida, previamente se debe realizar copias de respaldo de la información y brindar los roles de solo lectura a las entidades externas.

Cuando se transfiera información empleando web services, este debe ser consumido por usuarios y aplicaciones autorizadas, cuando se consuma información de un web service, este debe contar con los requisitos de seguridad que garanticen la seguridad de la información evitando la interceptación de la misma.

h) No están permitidos los reenvíos de información a cuentas de correo no autorizadas impidiendo la fuga de información de la entidad.

i) Se deben implementar procesos de inducción formativos a los funcionarios del CONSEJO PROFESIONAL sobre el correcto uso de la Información desde el momento de su ingreso a la entidad.

13.2.2 Acuerdos para la transferencia de información

Se deben establecer en los contratos con terceros las condiciones de manejo de información que provean confidencialidad, integridad y disponibilidad a la información Confidencial y de Uso Interno que se entregue o se reciba.

a) La Gerencia de Tecnologías de la Información y Telecomunicaciones del CONSEJO PROFESIONAL, apoyado en los procesos de Infraestructura TI y Seguridad de la Información y protección de datos, deben garantizar la seguridad en los medios de almacenamiento y trasmisión de la Información transmitidos por la entidad.

b) En la transmisión y recepción de la información el CONSEJO PROFESIONAL, debe solicitar formalmente la identificación de la persona o entidad antes de realizar entregas o envíos, validando la existencia de quien la solicita.

c) El CONSEJO PROFESIONAL, al entregar información debe brindar los requisitos mínimos de seguridad durante la entrega de la información, de la misma manera debe exigir a entidades externas estos mismos criterios de seguridad al recibir información, algunos de estos criterios se mencionan en el punto 10 de esta política.

d) Los criterios de garantía de la Información transferida se relacionan en esta política en los puntos 13.2.1 numeral b.

e) Las inconsistencias en la trasmisión de información, se deben reportar a las entidades externas pertinentes.

f) En caso de pérdida de información en la transmisión, esta debe ser reportada mediante el correo electrónico o la herramienta de mesa de ayuda al área de Tecnologías de la Información y Telecomunicaciones.

g) El CONSEJO PROFESIONAL, realiza la categorización de la Información durante la trasmisión la cual está descrita en el punto 8.2 de la presente política.

h) La información transmitida y decepcionada, debe ser registrada mediante el sistema físico o digital de gestión documental y basado en las tablas de retención implementadas por el CONSEJO PROFESIONAL.

i) El CONSEJO PROFESIONAL, mantendrá disponible la información durante todo el proceso de transmisión.

j) La cadena de custodia está determinada por en las tablas de retención de información establecidas por el CONSEJO PROFESIONAL.

k) Las medidas de protección para la transferencia de información en medios físicos se describen en el numeral 8.3.3 de esta política.

13.2.3 Mensajería Electrónica

a) El sistema de mensajería electrónica del CONSEJO PROFESIONAL oficialmente consiste en el servicio de correo electrónico corporativo el cual puede ser accedido por medio de correo.asmetsalud.com El proceso de Infraestructura Tecnológica es el encargado de garantizar el correcto funcionamiento de este servicio, al igual que deberá realizar las siguientes implementaciones de seguridad en las configuraciones del servidor de correo corporativo:

   Se deben comprobar los dominios de entidades externas. A través del sitio web https://www.mail-tester.com/

b) Los funcionarios internos del CONSEJO PROFESIONAL deben comprobar antes de enviar los mensajes, que el destinatario receptor sea quien dice ser.

c) El CONSEJO PROFESIONAL en el área de Tecnologías de la Información y Telecomunicaciones debe garantizar la confiabilidad y disponibilidad en el servicio de mensajería, en caso de ser a través de una entidad externa, se debe recurrir a los acuerdos de los niveles de servicio o ANS acordados.

d) Al ingresar el funcionario al el CONSEJO PROFESIONAL, en calidad de empleado se le asigna una dirección de correo electrónico con los accesos respectivos, el envío de mensajería electrónica, empleando este medió es categorizado como firma electrónica puesto que el empleado es identificado; Además es identificable el correo del remitente y del destinatario, teniendo validez como firma digital con los actos jurídicos según el decreto

2364 del año 2012. y la ley 527 del año 1999 en donde se da el reconocimiento jurídico a este tipo de mensajes de datos.

e) Los funcionarios del CONSEJO PROFESIONAL, deben solicitar al área de Tecnologías de la Información y Telecomunicaciones, los permisos correspondientes para utilizar servicios de mensajería instantánea pública como redes sociales.

f) Los niveles de autenticación permitidos por el CONSEJO PROFESIONAL para el acceso a redes públicas se definen alinear con los mencionados en el punto 9.2.4 de la presente política.

13.2.4 Acuerdo de confidencialidad o no divulgación

a) Las áreas de Servicios de Salud con apoyo del área Jurídica deberán realizar la implementación de minutas y/o cláusulas de acuerdos de confidencialidad o no divulgación de la información del CONSEJO PROFESIONAL evaluando el grado de confidencialidad descrito en el punto 8.2. de esta política; Dentro la información se puede relacionar la siguiente:

- Datos de la organización
- Datos personales de afiliados, empleados y contratistas
- Datos del CONSEJO PROFESIONAL relacionados a Información de manuales, instructivos, guías, formatos y relacionados
- Bases de datos
- Información de accesos al sistema de información y subsistemas y demás información relacionada con el CONSEJO PROFESIONAL.

b) El área de Tecnologías de la Información y Telecomunicaciones a través del proceso de Seguridad de la Información deberá velar porque los acuerdos de confidencialidad sean implementados, tanto para las partes internas (Empleados, colaboradores, etc.) como las partes externas (proveedores, aliados, etc.)

c) Los funcionarios de la entidad del CONSEJO PROFESIONAL y entidades externas, cuentan con un contrato de confidencialidad desde el inicio de su contratación, el cual termina cuando el funcionario interno o entidades externas terminan su contrato laboral con la entidad; El proceso retiro de accesos para los funcionarios de la entidad están descritos en esta política en los puntos 7.3.

d) Las responsabilidades relacionadas con la confidencialidad están dadas por los roles de revelador y receptor de la información transferida.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

14.1.1 Análisis y especificaciones de requisitos de seguridad de la información

Se debe involucrar Seguridad de la Información y protección de datos en el levantamiento de requerimientos y análisis de todo el proceso de adquisición, desarrollo y mantenimiento de los sistemas de información estableciendo los criterios de seguridad requeridos por la organización.

a) Se deben tener en cuenta los requisitos de seguridad como parte de los requisitos no funcionales, dentro del análisis y levantamiento de requerimientos de todo proceso de adquisición, desarrollo y mantenimiento de los sistemas.

   El proceso de Desarrollo Tecnológico, debe validar que los sistemas de información cuenten con tecnologías adecuadas que satisfagan los niveles de confianza en la autenticación y acceso de los usuarios de la Organización en ambientes de Desarrollo, Pruebas y Producción asignando credenciales de accesos junto con el link o ruta de pruebas vía correo electrónico.

b) Se debe realizar las validaciones correspondientes a procesos de autenticación de usuarios, procesos de suministros de accesos, privilegios y/o roles de usuarios.

   Se debe validar que los procesos de autenticación implementados sean gestionables a través de roles y privilegios.

c) Determinar la protección necesaria a los activos de información que se accederán tales como bases de datos, interacción con otros sistemas de información.

   El proceso de Gestión de Servicios debe informar a los usuarios, mediante correo electrónico con el asunto acuerdo de política de accesos sobre el correcto uso de los sistemas de información haciendo énfasis en sus deberes y responsabilidades.

d) Todo sistema de información debe tener un control de acceso de usuarios a través del directorio activo empresarial

   Se debe exponer las necesidades de protección requeridas para este activo de Desarrollo en relación a las posibles amenazas que pueden afectar la Confidencialidad, Integridad y Disponibilidad de las aplicaciones y desarrollos que componen el sistema de información.

e) Para el sistema de información en salud se debe validar que el/los usuarios autenticados estén activos en la base de datos de empleados.

   Se debe validar que a los usuarios del sistema de información le sean asignadas las credenciales de autenticación para el acceso al sistema, las credenciales de acceso son

intransferibles determinando así que cada registro de actividad o acción desarrollada dentro del sistema de Información, es responsabilidad del usuario poseedor de las credenciales de acceso siendo identificable y su responsabilidad irrefutable.

f) Se debe implementar en los sistemas de información interfaces de autenticación para el usuario y de ser necesario realizar validaciones en sistemas centralizados como directorios activos.

14.1.2 Seguridad de servicios de las aplicaciones en redes públicas.

a) El CONSEJO PROFESIONAL cuenta con diversos servicios corporativos que son necesarios poner a disposición de sus usuarios, por lo que se ve obligado a publicar servicios hacia internet de forma pública. Para garantizar la operación en esta actividad se dispone de sistemas unificados de amenazas y Firewall perimetral integrado – UTM, con los cuales se realizan las publicaciones activando sistemas de detección y prevención de intrusiones, AntiMalware y filtrado de servicios con el fin de salvaguardar la red corporativa y los sistemas de información y datos.

b) En la publicación de servicios también se consideran mecanismos de control en el acceso para el cumplimiento de las regulaciones del gobierno en materia de protección de datos personales, con los fines de salvaguardar la confidencialidad, integridad, disponibilidad de los datos.

Antes de publicar servicios web debe solicitarse las respectivas autorizaciones a las direcciones involucradas y contar con la autorización previa de los titulares de la información para el tratamiento de sus datos personales.

c) Para las redes VPN corporativas se implementan protocolos y certificados de seguridad que garantizan el aseguramiento de las conexiones y el tránsito de información en el acceso a la red interna del CONSEJO PROFESIONAL.

Las aplicaciones desarrolladas deben comunicar a las personas involucradas como proveedores, prestadores de servicios y afiliados el estado de las autorizaciones para el suministro o uso del servicio.

d) Se debe asegurar la confidencialidad e integridad de la información que publica y transita por las redes públicas garantizando la integridad de la información entre el revelador y receptor de la información mediante la asignación de credenciales de acceso y controles como los descritos en el punto 10 de esta política, estableciendo una responsabilidad irrefutable.

14.1.3 Protección de transacciones de los servicios de las aplicaciones

El área de Tecnología es responsable de los diversos servicios de aplicaciones corporativas que se tienen implementados en el Data Center principal y que componen el sistema de información del CONSEJO PROFESIONAL.

El consumo de los servicios de aplicación se realiza desde diversas zonas que componen la red corporativa, Redes LAN, DMZ, así como consumos a servicios de aplicación publicados. Por lo anterior se deberá garantizar la protección o salvaguarda de las transacciones de los servicios de aplicaciones para ello se implementan buenas prácticas de TI entre las cuales se pueden encontrar las siguientes.

- Certificados SSL y TLS, Protocolos de Encriptación
- Sesiones de usuario
- Autenticación de usuarios
- Conexiones VPN
- Segmentación de redes, segregación de VLANS
- UTM y Firewalls perimetrales, IDS/IPS,
- Otros no menos importantes.

14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

14.2.1 Política de desarrollo seguro

Se deben contemplar buenas prácticas de seguridad para el desarrollo seguro de software dentro del CONSEJO PROFESIONAL, entre las cuales se encuentran algunas mencionadas a continuación.

Se debe involucrar al proceso de Seguridad de la Información y Protección de Datos durante todo el ciclo de Desarrollo de Software revisando la implementación de controles de seguridad y buenas prácticas durante el desarrollo seguro dentro del CONSEJO PROFESIONAL.

a) El CONSEJO PROFESIONAL debe implementar ambientes de desarrollo y pruebas en su proceso de desarrollo interno in-house, los cuales se encuentran en la red interna de la entidad debidamente securizados.

b) Se debe contar con una metodología definida para llevar a cabo los desarrollos realizados.

c) Se deben contemplar requisitos de seguridad en la fase de diseño.

d) Se deben realizar las consideraciones necesarias de seguridad en la metodología de desarrollo de software. Al igual que los mecanismos de codificación seguras para lenguajes de programación utilizados.

   Se debe contar con chequeos de seguridad dentro de la ejecución del proyecto realizando Pruebas de Seguridad y Aceptación de Sistemas Desarrollados.

e) Se deben realizar procesos seguros en el control de versionamiento de software.

f) Se debe destinar en un repositorio definido por la organización la documentación electrónica del proyecto este proceso está descrito en el manual para el proceso de desarrollo de software SGI-DT-M-01 en el numeral 3.2.3 Estructura Documental.

g) Se debe contar con un control de versiona miento de los desarrollos.

h) Se debe conocer e implementar junto con el proceso de Seguridad de la Información y Protección de Datos, los requerimientos de seguridad de la información.

i) Se debe evidenciar todos los posibles errores encontrados en los sistemas desarrollados.

j) Se debe solicitar al proceso de Seguridad de la Información y Protección de Datos detectar las diferentes vulnerabilidades encontradas en los sistemas desarrollados y reportarlas mediante correo electrónico al proceso de Desarrollo entregando las recomendaciones necesarias para el tratamiento de estas.

14.2.2 Procedimientos de control de cambios en sistemas

a) Se deberán generar mecanismos para el adecuado control de cambios en el sistema de información del CONSEJO PROFESIONAL.

b) Las solicitudes de cambio en el sistema de información deben ser solicitadas a través de la herramienta de mesa de ayuda adjuntando el formato.

c) Se debe realizar las validaciones respectivas frente a solicitudes de cambios en el sistema de información relacionados con desarrollo de software In-House evitando posibles afectaciones relacionadas con la Confidencialidad, Integridad y Disponibilidad de la Información en el sistema ya implementado.

d) Se deben detallar los elementos de cambios dentro del procedimiento de control de cambios del sistema de información.

e) Se debe relacionar todos los elementos software, hardware, información, bases de datos inmersos en el procedimiento de control de cambios del sistema de información.

f) Se debe verificar el código crítico de seguridad de las aplicaciones desarrolladas y realizar las validaciones correspondientes en los ambientes de pruebas.

g) Se debe obtener aprobación formal para propuestas detalladas antes de iniciar un proceso de desarrollo.

h) Se antes de la implementación, debe asegurar que los usuarios autorizados acepten los cambios.

i) Se debe asegurar que el conjunto de documentación del sistema está actualizado al completar cada cambio, y que la documentación antigua se archiva, o se dispone de ella.

j) Se debe mantener un control de versiones para todas las actualizaciones de software.

k) Se debe mantener un rastro de auditoría (Audit Trail) de todas las solicitudes de cambio.

l) Se debe asegurar que la documentación de la operación (véase el numeral 12.1.1) y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados.

m) Se debe asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados.

14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

a) Cuando se realicen cambios en las aplicaciones se deben realizar revisiones técnicas de las mismas con el fin de asegurar que no haya impactos adversos en las actividades y operaciones del CONSEJO PROFESIONAL. Esta actividad debe ser realizada por el área de Tecnologías de la Información y Telecomunicaciones.

b) El Profesional de Gestión de Servicios y su equipo deberán realizar oportunamente las notificaciones a los usuarios de la aplicación correspondiente a cambios en los sistemas de información, plataformas, aplicaciones y servicios de TI.

c) El área de Tecnologías de la Información y Telecomunicaciones debe asegurar que los cambios realizados en las plataformas tecnológicas productivas se ajusten a los planes de continuidad del negocio, este proceso se describe en el punto 17.1.3 de esta política.

14.2.4 Restricciones en los cambios a los paquetes de software

a) Los usuarios tienen prohibido realizar cambios en el software instalado por el área de Tecnologías de la Información y Telecomunicaciones en las estaciones de cómputo y otros dispositivos, esto con el fin de prevenir riesgos en la integridad de la información. Para hacer cumplir esta política el área de Tecnologías de la Información y Telecomunicaciones implementa controles de seguridad a través del servidor dominio de equipos principal.

b) Los cambios en los paquetes de software que, por razones de mejora o requerimientos específicos de las necesidades de los usuarios, para el desarrollo de actividades de la labor diaria pueden ser aplicados con el acompañamiento del proceso de Infraestructura Tecnológica previa solicitud formal a través de la herramienta de mesa de ayuda.

En cuanto a las instalaciones de paquetes software que extienden o mejoran las características y seguridad de los programas o aplicaciones informáticas como parches de seguridad, framework, actualizaciones o el uso de librerías; Estas sólo serán admitidas si son obtenidas directamente de los vendedores o proveedores fabricantes de las tecnologías, obteniendo los medios de instalación de sus repositorios oficiales.

El proceso de instalación de los paquetes de software los cuales corrigen las vulnerabilidades en los sistemas informáticos que se describen en el punto 12.6.1 en el literal d, de esta política.

Se debe tener el previo conocimiento de los paquetes software a instalar antes de ser aplicados en el programa estándar.

c) Se debe documentar el proceso de instalación de los paquetes software aplicados, con el fin de poder realizar mantenimientos futuros de manera independiente si el impacto ha sido positivo.

d) Una vez aplicados los paquetes software en las aplicaciones informáticas, se debe revisar la compatibilidad con otros sistemas informáticos de la entidad.

14.2.5 Principios de construcción de sistemas seguros

A continuación, se definen los primordiales principios de construcción de sistemas seguros en EL CONSEJO PROFESIONAL. El área de Tecnologías de la Información y Telecomunicaciones es libre de incorporar otros principios que aporten a la seguridad en la construcción de los sistemas.

a) En los procesos de análisis y diseño se definen los roles que tendrán acceso a los diferentes módulos del sistema.

b) En la capa interfaz y negocio se deben definir las validaciones acordes a cada nivel.

c) En la creación de módulos nuevos se debe tener en cuenta que estos solo pueden ser accedidos por medio de roles del sistema existentes o nuevos si es necesario.

d) En la creación de módulos nuevos se deben crear prototipos y ser validados por los clientes para establecer si es lo que realmente se necesita a nivel de FrontEnd.

e) Los cambios solicitados deben ser documentados por medio de los formatos definidos en los procesos aprobados para el desarrollo de software.

14.2.6 Ambiente de desarrollo seguro

El proceso de Infraestructura Tecnológica en conjunto con Seguridad de la Información y Protección de Datos, deberán diseñar e implementar los ambientes de desarrollo seguro durante todo el ciclo, minimizando los riesgos asociados a las labores de desarrollo,

a) Se debe asegurar la protección de los datos que se van a procesar, almacenar y transmitir en el cumplimiento de las leyes y regulaciones aplicables, transacciones de datos, del código fuente, y entre otras consideraciones basadas en buenas prácticas en el desarrollo de software.

b) Se debe durante todo el ciclo de desarrollo debe realizar una valoración de los riesgos generados producto de la construcción de aplicaciones que cumplan con los requisitos internos y externos pero que a su vez se exponga la seguridad de la información en la CID.

c) Se debe aplicar los controles de seguridad ya implementados por la organización, que brindan soporte al desarrollo del sistema.

d) Se debe valorar el riesgo asociado al factor humano en la confiabilidad del personal que trabaja en el ambiente de desarrollo.

e) Se debe incluir la utilización y buenas prácticas en los ambientes de desarrollo seguro en los acuerdos de contratación externa si se llegase a presentar.

f) Se debe separar los diferentes ambientes de desarrollo de acuerdo a factores relacionados con los proyectos como la inmediatez, tipo, alcance entre otros.

g) Los controles de acceso en los ambientes de desarrollo deben ser gestionados por el proceso de Desarrollo y autorizados por el coordinador de Desarrollo; quien debe realizar la asignación del ambiente de desarrollo al recurso humano que trabaja en él.

h) Se debe realizar el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí empleando repositorios de almacenamiento on premise o en cloud;

i) Se deben realizar las copias de respaldo y almacenar en lugares seguros fuera del sitio on premise o cloud;

j) Se debe tener un control sobre el movimiento de datos desde y hacia el ambiente, este proceso lo debe realizar solicitando bases de datos para desarrollo, a TI.

14.2.7 Desarrollo contratado externamente

Cuando se requieran desarrollos externos para el CONSEJO PROFESIONAL se deben cumplir con las siguientes directrices de seguridad.

a) En los contratos para desarrollos externos se deben implementar acuerdos de licenciamiento, propiedad del código fuente y derechos de propiedad intelectual. Así mismo cláusulas de confidencialidad, no divulgación y privacidad para la protección de datos personales y protección de datos corporativos, derechos de uso, cláusulas de destrucción o devolución de la información del CONSEJO PROFESIONAL que fue suministrada una vez se termine el contrato. Esto debe ser implementado por el proceso de Contratación apoyado con el área Jurídica.

b) Para la contratación de desarrollos externos o servicios de TI que las áreas requieran es de obligatoriedad consultar al área de Tecnologías de la Información y Telecomunicaciones para garantizar que los desarrollos o servicios de TI que van a ser contratados se incorporen o integren adecuadamente a la infraestructura tecnológica y sistemas de información el

CONSEJO PROFESIONAL, así como también a buenas prácticas de seguridad y tecnologías de la información que se vean necesarias.

14.2.8 Pruebas de seguridad de sistemas

a) Las pruebas de seguridad durante el ciclo de desarrollo de los sistemas serán ejecutadas por el proceso de Seguridad de la Información y Protección de Datos acorde con el análisis de vulnerabilidades en la gestión de la vulnerabilidad técnica, ver numeral 12.6.1.

b) Se debe solicitar al proceso de Seguridad de la Información y Protección de Datos el respectivo análisis de vulnerabilidades en los sistemas de pruebas antes de salir a producción, estos análisis deben ser enviados vía correo electrónico al Proceso de Desarrollo Tecnológico.

c) Las pruebas de seguridad de sistemas también pueden ser ejecutadas por proveedores externos competentes bajo el acompañamiento de la interventoría de contratos y/o el proceso de Seguridad de la Información y Protección de Datos.

14.2.9 Prueba de aceptación de sistemas

Las pruebas de aceptación se contemplan para los sistemas de información nuevos, actualizaciones y/o nuevas versiones se contemplan las siguientes directrices:

a) Se deben crear y ejecutar planes de pruebas de aceptación acorde con los requerimientos que se hayan definido inicialmente y en donde el cliente defina si acepta o no las pruebas de aceptación.

b) Las aprobaciones de pruebas de aceptación deberán diligenciarse a través de los formatos Aprobación de las Pruebas de Aceptación y formato para el registro de pruebas de seguridad.

14.3 DATOS DE PRUEBA

14.3.1 Protección de datos de prueba

a) Los datos de pruebas para el desarrollo del CONSEJO PROFESIONAL deben ser tomados de bases de datos obsoletas y en lo posible realizar intercambios de datos aleatoriamente entre registros.

b) Los datos de pruebas para desarrollo deben ser actualizados mediante mesa de ayuda

c) Las políticas de protección de datos personales y datos corporativos también son aplicables en la salvaguarda o protección de datos de pruebas utilizados en desarrollo.

15. RELACIONES CON LOS PROVEEDORES

15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

15.1.1 Seguridad de la información para las relaciones con proveedores

a) En los contratos con proveedores y/o aliados externos se deben implementar cláusulas de confidencialidad, no divulgación y privacidad para la protección de datos personales y protección de datos corporativos, derechos de uso de información, cláusulas de destrucción o devolución de la información del CONSEJO PROFESIONAL que fue suministrada una vez se termine el contrato. Esto debe ser implementado por el proceso de Contratación apoyado con el área Jurídica.

b) Los procesos a través del personal que haga de interventores de contratos o alianzas deben poner a disposición la presente política de seguridad a las partes externas.

15.1.2 Tratamiento de la seguridad dentro de acuerdos con proveedores

Los procesos deberán establecer y documentar las relaciones con proveedores que puedan tener acceso, procesar, comunicar, almacenar o suministrar componentes de infraestructura de TI para el sistema de información del CONSEJO PROFESIONAL bajo los lineamientos establecidos por la organización y adicionalmente debe considerar los siguientes aspectos.

- Descripción de la información que se va a suministrar o a la que se va a acceder. Medios de accesos.
- Clasificación de acuerdo con el esquema de clasificación corporativo.
- Requisitos legales y de reglamentación, incluida la protección de datos personales, derechos autor y de propiedad intelectual.
- Se deben acordar grupos de controles de acceso a la información.
- Entre otros que se consideren importantes.

15.1.3 cadena de suministro de tecnología de información y comunicación

a) Las áreas dentro de acuerdos con proveedores (proveedores de productos o servicios de tecnologías de la información y comunicación) deben establecer requisitos para tratar los riesgos de seguridad de la información asociados.

b) Se deberá exigir a los proveedores que entreguen o divulguen buenas prácticas de seguridad relacionadas a los productos o servicios suministrados.

c) Se debe exigir manuales de uso de los productos y servicios, con las consideraciones de seguridad para mantener la funcionalidad de los productos y servicios.

d) En relación a los productos y servicios se debe establecer reglas de comunicación con proveedores con el fin de evitar inconvenientes, lograr la resolución de problemas oportunamente, lograr informar sobre funcionamientos.

15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES

15.2.1 Seguimiento y revisión de los servicios de los proveedores

Los servicios prestados por proveedores deberán ser monitoreados y revisados con el fin de que se cumplan los términos y condiciones de seguridad de la información, y que se resuelvan incidentes y problemas de forma oportuna y eficiente.

En relación al seguimiento y revisión se debe considerar niveles de desempeño, gestión de la capacidad del servicio por parte del proveedor, resolución de problemas identificados, entre otros aspectos relacionados.

15.2.2 Gestión de cambios en los servicios de los proveedores

Se debe gestionar una adecuada gestión de cambios de servicios de los proveedores en base a seguimientos, revisiones de servicios y cumplimientos de los requerimientos exigidos, o también por los cambios de mejora informados por parte de proveedores. En este proceso se deben considerar.

- Cambios en los acuerdos con los proveedores
- Cambios realizados por la organización para implementar
- Cambios en los servicios de los proveedores para implementar

16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN

16.1.1 Responsabilidades y procedimientos

a) La gestión de incidentes de seguridad de la información es responsabilidad del proceso de Seguridad de la Información.

16.1.2 Reporte de eventos de seguridad de la información

a) Los usuarios deben reportar los eventos e incidentes de seguridad a través de la herramienta de mesa de ayuda o enviando un correo electrónico a informatica@consejoprofesionalmvz.gov.co con copia al correo registro@consejoprofesionalmvz.gov.co

El Profesional Administrador SGSI determinará la categoría respectiva, lo asignará al equipo indicado de resolución, lo escalará a las áreas de control si así se requiere e informará a quienes sea pertinente.

b) En la identificación y reportes de eventos se deben considerar los siguientes aspectos:

- Violaciones de acceso y Errores humanos
- Violaciones de la integridad, confidencialidad y disponibilidad de la información
- No cumplimientos de políticas y directrices
- Violaciones de la seguridad física y otros relacionados a seguridad.

c) Las investigaciones especiales adelantadas por los entes de control relacionadas con la seguridad de la información deben ser notificadas al proceso de Seguridad de la Información.

16.1.3 Reporte de debilidades de seguridad de la información

Los funcionarios del CONSEJO PROFESIONAL, contratistas y usuarios del sistema que observen situaciones sospechosas o que claramente sean incidentes de seguridad de la información tienen la obligación de reportarlo al proceso de Tecnologías de la Información y Telecomunicaciones. Enviando un correo electrónico a informatica@consejoprofesionalmvz.gov.co con copia a la cuenta registro@consejoprofesionalmvz.gov.co.

16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos

a) Los eventos serán evaluados para la identificación de amenazas y mitigar la materialización de las mismas, esto será llevado a cabo por el proceso de Seguridad de la Información apoyado con los demás colaboradores del área de Tecnologías de la Información y Telecomunicaciones y procesos involucrados.

b) En la documentación de evaluaciones de eventos y resolución de los mismos se detallará el evento, así como las acciones tomadas frente a los mismos.

16.1.5 Respuesta a incidentes de seguridad de la información

El área de Tecnologías de la Información y Telecomunicaciones en apoyo con las áreas involucradas en incidentes de seguridad de la información dará respuesta a los mismos acordes con el manual de gestión de incidentes.

16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información

Todos los incidentes deberán ser registrados en la herramienta de mesa de ayuda, con el fin de llevar un control sobre los mismos, así como de poder registrar las resoluciones de los mismos como

estrategia de aprendizaje. También para lograr observar incidentes comunes y tomar acciones diferentes que resulten más afectivas.

16.1.7 Recolección de evidencia

El equipo de seguridad deberá realizar la recolección de evidencia considerando:

- Cadena de custodia
- Sesiones informativas
- Seguridad del personal
- Roles y responsabilidades personal involucrado
- Seguridad de la evidencia
- Competencia del personal y Documentaciones

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

17.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN

17.1.1 Planificación de la continuidad de la seguridad de la información

Se planifica la continuidad de los servicios de TI en donde se incluye la continuidad de seguridad de la información.

El proceso de Seguridad de la Información y Protección de Datos Personales implementa la IRBC (Preparación de las TIC para la continuidad de negocio.) como un elemento estratégico en la compañía que soporta el BCP (Plan de Continuidad del Negocio) y los procesos del SGSI.

La IRBC inicia con el análisis de impacto al negocio desde el área de Tecnologías de la Información y Telecomunicaciones (BIA de TI), pasa por el establecimiento y apropiación de estrategias de continuidad y termina con el seguimiento del cumplimiento y mejora de las mismas. La IRBC es aplicable en el CONSEJO PROFESIONAL, a los servicios TIC gestionados por el área de Tecnologías de la Información y Telecomunicaciones, y es liderada por la coordinación de seguridad de la información, con el apoyo de las coordinaciones de infraestructura y desarrollo.

La IRBC aporta como beneficio a la compañía tener la resiliencia suficiente para enfrentar posibles situaciones adversas, minimiza los impactos financieros y reputacionales de las mismas, brinda confianza adicional a las estrategias de continuidad de negocio, entre otros.

17.1.2 Implementación de la continuidad de la seguridad de la información

a) La implementación de la continuidad de la seguridad de la información está liderada por el proceso de Seguridad de la Información y Protección de Datos Personales y es apoyada por el proceso de Infraestructura de TI y Desarrollo Tecnológico.

b) El área de Tecnologías de la Información y Telecomunicaciones conforma un equipo de respuesta a incidentes de seguridad de la información y protección de datos personales, en adelante ISIRT, Information Security Incident Response Team por sus siglas en inglés, el cual se enfoca en evaluar y responder a los eventos, incidentes y vulnerabilidades de seguridad de la información que puedan afectar significativamente directa e indirectamente los servicios tecnológicos dentro del CONSEJO PROFESIONAL, se busca aprender de ellos, gestionarlos, reducir el daño económico y reputacional de la organización, retroalimentar e informar a las partes interesadas.

c) Se debe desarrollar y aprobar planes, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle cómo la organización gestionará un evento perturbador y mantendrá su seguridad de la información en un nivel predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobada por la dirección (véase el numeral 17.1.1).

d. Ante situaciones adversas se deberá implementar mecanismos contingentes en pro de garantizar la continuidad de la seguridad de la información. Por lo anterior se implementarán Firewalls y herramientas que ayuden a este fin.

e. Los planes especificados en el Plan de Contingencia y Continuidad se deberán someter a pruebas al menos una vez al año, para asegurar su actualización y su eficacia. Asimismo, el Plan de Contingencia y Continuidad debe ser revisado al menos una vez al año y actualizado si en la revisión se detecta que se requiere.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

a) En tiempos planificados el proceso de Seguridad de la Información con apoyo del área de Tecnología verificará, revisará y evaluará las estrategias de continuidad de la seguridad de la información.

17.2 REDUNDANCIAS

17.2.1 Disponibilidad de instalaciones de procesamiento de información

El CONSEJO PROFESIONAL conocedora de la importancia de las instalaciones del centro de datos de procesamiento de información dispone de un sitio alterno para mantener la disponibilidad de instalaciones de procesamiento de datos e información y mantener la continuidad de las operaciones. Para lo anterior mencionado se pone a disposición el Plan de Recuperación de Desastres (DRP).

a) El proceso de Seguridad de la Información deberá proveer de los mecanismos para mantener la seguridad de los sitios redundantes del CONSEJO PROFESIONAL.

18. CUMPLIMIENTO

18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales.

a) El proceso de Seguridad de la información es responsable de mantenerse al tanto sobre la legislación aplicable de seguridad de la información y seguridad informática a través del normograma estipulado por el área Jurídica.

b) El área jurídica debe brindar asesoría respectiva en la implementación de políticas y controles que ayuden al cumplimiento de las leyes y regulaciones.

c) El proceso de Seguridad de la Información deberá investigar sobre legislación aplicable y estar consultando al área Jurídica sobre el tema.

d) El proceso de Seguridad de la Información deberá apoyarse con el área Jurídica para las revisiones de la legislación aplicable sobre seguridad de la información.

18.1.2 Derechos de propiedad intelectual.

a) Todo material utilizado por el CONSEJO PROFESIONAL debe ser adquirido cumpliendo con los requisitos legales. Para la instalación de Software en equipos adquiridos por terceros se debe solicitar por parte del área de Tecnologías de la Información y Telecomunicaciones certificación del tercero de que el software ha sido adquirido legalmente y cumple con las obligaciones relativas a los derechos de propiedad intelectual.

b) Todo funcionario del CONSEJO PROFESIONAL y partes relacionadas, son responsables de garantizar que todo el material que utilicen con propósito laboral cumple con la legislación de derechos de propiedad intelectual.

c) Está prohibido que usuarios finales instalen software en los computadores de la Entidad; esta función es exclusiva del área de Tecnologías de la Información y Telecomunicaciones, quien debe tener un control de las licencias de los programas de software y velar porque no exista software sin la debida licencia de uso.

d) Únicamente el área de Tecnologías de la Información y Telecomunicaciones está autorizada para tomar una copia con propósito de respaldo de los medios originales de los programas de software licenciados.

e) La instalación por parte de funcionarios del CONSEJO PROFESIONAL o terceras partes de programas de software en los computadores de la Entidad sin la debida autorización es considerado como un incidente de seguridad.

f) Los funcionarios del CONSEJO PROFESIONAL y terceras partes, no deben descargar o almacenar archivos de música, fotos, vídeos, o material sujeto a propiedad intelectual en los equipos del CONSEJO PROFESIONAL sin autorización del propietario.

g) Los funcionarios del CONSEJO PROFESIONAL y terceras partes no deben, por ningún motivo, descargar, instalar, almacenar o utilizar herramientas de software o hardware como crackers de software, software de descubrimiento de contraseñas, detección de vulnerabilidades o utilidades de cifrado no autorizadas que puedan ser utilizadas para evaluar o comprometer los sistemas de seguridad de la información, sin la autorización del proceso de Seguridad de la Información.

h) Se debe incluir en el programa de concientización de seguridad de la información el cumplimiento de las leyes de propiedad intelectual.

18.1.3 Protección de registros

a) Los registros sobre requisitos legislativos, de reglamentación, contractuales y de negocio que deberán ser almacenados y custodiados de forma segura por parte de cada proceso.

b) Los registros que se consideren importantes y que de acuerdo a las directrices de cada proceso sea necesario deben ser almacenados en forma física y digital a través de los sistemas de información y herramientas que se hayan definido.

18.1.4 Protección de los datos y privacidad de la información relacionada con los datos personales.

a) En atención a la Ley 1581 de 2012 y sus decretos reglamentarios se ha establecido la Política de Protección de Datos Personales y el aviso de privacidad cuyo cumplimiento es obligatorio bajo este numeral de la política de seguridad y por las exigencias de la ley.

b) Se implementa el Programa Integral de protección de datos bajo las recomendaciones estipuladas por el ente de control Superintendencia de Industria y Comercio.

c) Las áreas deberán realizar lo respectivo al cumplimiento de la ley 1581 de 2012 y sus decretos reglamentarios referente a las autorizaciones por parte de afiliados, empleados, proveedores y otros relacionados en el tratamiento de datos personales.

18.1.5 Reglamento de controles criptográficos

Se deberán implementar controles criptográficos en los casos que se requiera para preservar la seguridad de la información de los datos. Lo anterior con los fines de cumplimiento de acuerdos, legislación y reglamentaciones pertinentes.

18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

18.2.1 Revisión independiente de la seguridad de la información

a) El proceso de Seguridad de la Información deberá gestionar las revisiones independientes de la seguridad de la información al menos una vez cada año a partir de la fecha de aprobación de la presente directriz y política de seguridad.

b) Las revisiones independientes pueden realizarse por actores relacionados con la seguridad de la información tales como empresas, consultores externos, grupos de investigación, investigadores independientes y comunidades. Lo anterior bajo el cumplimiento de la ley y las estipulaciones contractuales o de cooperación.

c) El proceso de Seguridad de la Información deberá revisar supervisión, interventoría y acompañamiento a las revisiones independientes de seguridad de la información.

18.2.2 Cumplimiento con las políticas y normas de seguridad

La Presidencia, Secretaría y Coordinadores de procesos deberán revisar con frecuencia el cumplimiento de las presentes políticas, lineamientos, directrices y buenas prácticas dentro de su área de responsabilidad con las presentes políticas y de cualquier otro requisito de seguridad de la información.

18.2.3 Revisión de cumplimiento técnico

Se debe revisar periódicamente las configuraciones en los componentes de infraestructura de tecnologías de la información y la comunicación del sistema de información en pro de validar que estén acordes con el cumplimiento técnico de políticas de seguridad de la información.
Se deberá realizar análisis de vulnerabilidades y Pentesting para verificar configuraciones basadas en buenas prácticas de TI en relación al cumplimiento técnico.

19. DUDAS Y RECOMENDACIONES

Con el fin de poder responder las dudas, comentarios o sugerencias generadas por este documento, podrá comunicarse al correo electrónico informatica@consejoprofesionalmvz.gov.co con copia a registro@consejoprofesionalmvz.gov.co colocando como asunto: “Política de Seguridad”.

	EMISIÓN		
	ELABORÓ	**REVISÓ**	**APROBÓ**
Nombre:	**TD Technodigital S.A.S.**	**Andres Herrera Garcia**	**Liliana Muñoz Pineda**
Cargo:	**Firma Externa**	**Asistente de Registro Profesional**	**Secretaria Ejecutiva**
Firma:			