Tabla de Contenido

1. INTRODUCCIÓN 6

2. OBJETIVOS 6

3. ALCANCE DEL DOCUMENTO 6

4. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 7

***OBJETIVOS*..... 7**

***ALCANCE*..... 7**

***NIVEL DE CUMPLIMIENTO*..... 8**

5. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN..... 9

5.1 MANUAL DE POLÍTICAS 9

5.2 OBJETIVOS 9

5.3 ALCANCE 10

5.4 NIVEL DE CUMPLIMIENTO 10

5.5 NORMATIVIDAD PERTINENTE 11

5 5.1 Normas que rigen para la estructura organizacional de seguridad de la información11

5.5.2 Normas para uso de dispositivos móviles..... 12

5.5.3 Normas para uso de conexiones remotas 14

5.5.4 Normas relacionadas con la vinculación de funcionarios 15

5 5.5 Normas aplicables durante la vinculación de funcionarios y personal provisto por terceros 15

5.5.6 Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros 1 6

5.5..7 Normas de responsabilidad por los activos de información 17

5.5.8 Normas para la clasificación y manejo de la información..... 19

5.5.9 Normas uso de periféricos y medios de almacenamiento 20

5.5.10 Normas de acceso a redes y recursos de red..... 21

5.5.11 Normas de administración de acceso de usuarios..... 22

5.5.12 Normas de responsabilidades de acceso de los usuarios..... 23

5.5.13 Normas de uso de altos privilegios y utilitarios de administración..... 23

5.5.14 Normas de control de acceso a sistemas y aplicativos 24

5.5.15 Normas de controles criptográficos 26

5.5.16 Normas de áreas seguras..... 27

5.5.17 Normas de seguridad para los equipos institucionales..... 29

5.5.17 Normas de asignación de responsabilidades operativas 31
5.5.18 Normas de protección frente a software malicioso 32
5.5.19 Normas de copias de respaldo de la información 33
5.5.20 Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de

información 34
5.5.21 Normas de control al software operativo 35
5.5.22 Normas para la gestión de vulnerabilidades 35
5.5.23 Normas de gestión y aseguramiento de las redes de datos 36
5.5.24 Normas de uso del correo electrónico 37
5.5.25 Normas de uso adecuado de internet 38
5.5.26 Normas de intercambio de información 39
5.5.27 Normas para el establecimiento de requisitos de seguridad 41
5.5.28 Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas ... 42
5.5.29 Normas para la protección de los datos de prueba 45
5.5.30 Normas de inclusión de condiciones de seguridad en la relación con terceras partes 45
5.5.31 Normas de gestión de la prestación de servicios de terceras partes 46
5.5.32 Normas para el reporte y tratamiento de incidentes de seguridad 47
5.5.33 Normas de redundancia 48
5.5.34 Normas de cumplimiento con requisitos legales y contractuales 48
5.5.35 Normas de privacidad y protección de datos personales 49
5.6 RESPONSABILIDADES 50

6 PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN 51

6.1 PROCEDIMIENTO DE ASIGNACIÓN DE EQUIPOS Y ACCESO A SISTEMAS DE INFORMACIÓN 51
6.2 OBJETIVO GENERAL 51
6.3 ALCANCE 52
6.4 RESPONSABILIDADES 52
LA DEPENDENCIAS DEL IMRDS 52
RECURSOS HUMANOS 52
SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA 52
LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA 52
6.4.5. USUARIOS DE SISTEMAS DE INFORMACIÓN 53
6.5 DESCRIPCIÓN DEL PROCEDIMIENTO 54
INVENTARIO DE ACTIVO FIJO TECNOLÓGICO 54
ASIGNACIÓN DE EQUIPOS Y CREACIÓN DE CUENTAS 54
ACCESO A SISTEMAS DE INFORMACIÓN 55
DEVOLUCIÓN DE ACTIVOS Y DES HABILITACIÓN DE CUENTAS 55
6.6 INSTRUCTIVOS Y PROCEDIMIENTOS 56
INSTRUCTIVO DE USO DE COMPUTADORES PERSONALES 56
PROCEDIMIENTO DE DESARROLLO Y ACTUALIZACIÓN DE SISTEMAS DE INFORMACIÓN 57

INTRODUCCIÓN 57
OBJETIVO GENERAL 58
6.6.1.1 ALCANCE 58
RESPONSABILIDADES 58
LAS DEPENDENCIAS DEL IMRDS 58
6.6.1.2 LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA 58

6.6.2.6 ROLES ESPECÍFICOS 59
6.6.2.7. DESARROLLO DE NUEVOS SISTEMAS DE INFORMACIÓN 60
SOLICITUD DE REQUERIMIENTOS 60
ESPECIFICACIÓN DE REQUERIMIENTOS 60
PLAN DE PROYECTO 61
CONSTRUCCIÓN 61
PRUEBAS 62
PASO A PRODUCCIÓN 63
PASOS POSTERIORES A PASO A PRODUCCIÓN 64
CAMBIOS DE EMERGENCIA – ERROR DE SISTEMA 64
NOTIFICACIÓN Y ASIGNACIÓN 64
PRUEBAS 64
PASO A PRODUCCIÓN 65
MEJORAS DE SISTEMA 65
NOTIFICACIÓN Y ASIGNACIÓN 65
PRUEBAS 65
PASO A PRODUCCIÓN 66
CAMBIOS MAYORES DE SISTEMAS 66
ESTÁNDARES DE DESARROLLO 66
LENGUAJE DE PROGRAMACIÓN 66
BASES DE DATOS 66
GESTIÓN DE CÓDIGO FUENTE 66
DEFINICIÓN DE AMBIENTES 67
6.7 PROCEDIMIENTO DE RESPALDOS DE LA INFORMACIÓN 73
6.7.1 Introducción 73
6.7.2 Objetivo general 74
6.7.3 Alcance 74
6.7.4 Responsabilidades 74
la oficina de gestión tecnológica e informática 74
personal del IMRDS 74
6.7.5 Descripción del procedimiento 74
Consideraciones generales 74
Medios de respaldo 75
Recuperación 75

6.8 PROCEDIMIENTO DE SEGURIDAD DE OFICINAS E INSTALACIONES 75
6.8.1 Introducción *75*
6.8.2 Objetivo *76*
6.8.3 Alcance *76*
6.8.4 Responsabilidades *76*
La oficina de gestión tecnológica e informática 76
Personal del IMRDS 76
6.8.5 Descripción del procedimiento *76*
Acceso a oficinas del IMRDS 76
Acceso a servidores y equipos de comunicaciones 77
Acceso a bodega informática 77
6.9. PROCEDIMIENTO DE SEGURIDAD DE REDES 77
6.9.1. Introducción *77*
6.9.2. Objetivo *77*
6.9.3. Alcance *77*
6.9.4. Responsabilidades *77*
6.9.4.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA 77
6.9.4.2. Personal del IMRDS 78
6.9.5. Descripción del procedimiento *78*
6.9.5.1. Terminología 78
6.9.5.2. Administración de la red y de equipos de conectividad 78
6.9.5.3. Acceso lógico al dominio LOCAL 79
6.9.5.4. Acceso lógico a los sistemas de información 80
6.9.5.5. Administración del acceso remoto (VPN) 80
6.9.5.6. Acceso lógico al punto de acceso inalámbrico (WIFI) 80
6.9.5.7. Seguridad del cableado y protección a los puertos de red 80
6.10. PROCEDIMIENTO DE GESTIÓN DE INCIDENTES, AMENAZAS Y DEBILIDADES DE SEGURIDAD 81
6.10.1. Introducción *81*
6.10.2. Objetivo *81*
6.10.3. Alcance *81*
6.10.4. Responsabilidades *81*
6.10.4.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA 81
6.10.4.2. Personal del IMRDS 82
6.10.5. Descripción del procedimiento *82*
6.10.5.1. Activos de información y tipos de incidentes 82
6.10.5.2. Reporte de incidentes, amenazas y debilidades de seguridad 82
6.10.5.3. Respuesta ante incidentes, amenazas y debilidades de seguridad 83
6.11. PROCEDIMIENTO DE MONITOREO DE RED Y SERVICIOS 83
6.11.1. Introducción *83*
6.11.2. Objetivo *83*
6.11.3. Alcance *83*

6.11.4. Responsabilidades 84
6.11.4.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA 84
6.11.4.2. Personal del IMRDS 84
6.11.5. Descripción del procedimiento 84
6.12. PROCEDIMIENTO DE OPERACIONES DEL CENTRO DE DATOS 85
6.12.1. Introducción 85
6.12.2. Objetivo 85
6.12.3. Alcance 85
6.12.4. Responsabilidades 85
6.12.4.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA 85
6.12.4.2. Personal de laIMRDS 85
6.12.5. Descripción del procedimiento 86
6.12.5.1. Sistema Eléctrico y respaldo de energía mediante UPS 86
6.12.5.2. Sistema de enfriamiento (Aire acondicionado) 86
6.12.5.3. Enlace de Internet, MPLS y telefonía 87
6.12.5.4. Equipos de comunicaciones 87
6.12.5.5. Equipos de servidores y cluster de virtualización 87
6.12.5.6. Equipo Storage 88
6.13. PROCEDIMIENTODEACTUALIZACIÓNDESISTEMASOPERATIVOSYSOFTWARE 88
6.13.1. Introducción 88
6.13.2. Objetivo 88
6.13.3. Alcance 88
6.13.4. Responsabilidades 88
6.13.4.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA 88
6.13.4.2. Personal del IMRDS 88
6.13.5. Descripción del procedimiento 89
6.13.5.1. Sistemas Operativos de Servidores 89
6.13.5.2. Sistemas Operativos de PC a funcionarios 89
6.13.5.3. Software de los servidores 89
6.14. Procedimiento de Aplicación y Control de Firmas Digitales Introducción 90
6.14.1. Objetivo 90
6.14.2. Alcance 90
6.14.3. Responsabilidades 90
6.14.3.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA 90
6.14.3.2. Personal del IMRDS 90
6.14.4. Descripción del procedimiento 90

7. ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 91

8. INVENTARIO DE ACTIVOS DE INFORMACIÓN 93

8.1 RESPONSABILIDAD 94
8.2 INVENTARIO DE ACTIVOS 95
8.3 ROTULADO DE LA INFORMACIÓN 95
8.4 CLASIFICACIÓN DE LA INFORMACIÓN 95
8.4.1 Confidencialidad 95
8.4.2 Integridad 96
8.4.3 Disponibilidad 96

1. INTRODUCCIÓN

A través de los años se ha sostenido la infraestructura tecnológica solo con fines de prestar y mantener un servicio a usuarios dando el mejor soporte a ellos, pero en la actualidad esos esfuerzos ya no son suficientes para conservar y preservar de forma segura la información en los entornos corporativos, debido a que la tecnología, el conocimiento y los riesgos se han desarrollado de manera exponencial lo cual ha llevado a las entidades gubernamentales y privadas a incrementar las inversiones en elementos, equipos y profesionales para la implementación de sistemas que permitan estar a la vanguardia de los retos que deben ser afrontados como respuesta a la evolución.

2. OBJETIVOS

- Generar pautas para la prestación de servicios a la comunidad de forma continua e interrumpida en el IMRDS.
- Fomentar el uso y apropiación de la Política de Seguridad vigente en los funcionarios y contratistas del IMRDS.
- Reducir las brechas de seguridad, de forma ordenada y guiada por los parámetros dictaminados desde el Ministerio de las TIC's.
- Establecer políticas que mejoren los servicios prestados mediante tecnologías de la información a las dependencias dentro de la entidad, procurando la mejora continua y optimización de los procesos.
- Crear un grupo de investigación enfocado al análisis de las necesidades y brechas de Tecnología de la Información que se presentan en el municipio, formulando e implementando proyectos que impacten desde el IMRDS a empresarios, comunidades de los sectores públicos y privados.

3. ALCANCE DEL DOCUMENTO

El presente documento está enfocado en mejorar la estrategia para el análisis, diseño, ejecución y control de los proyectos gestados desde el área de tecnología, aplicables a la adopción de sistemas de información para mejorar los canales de comunicación, participación, opinión, percepción, uso y apropiación de los servicios brindados por el IMRDS conforme a los dominios del marco de referencia; involucrando y prestando apoyo a todos los usuarios que tengan interacción con los servicios tecnológicos facilitados por la entidad durante el periodo (2024-2027), logrando una comunicación interna eficiente entre todas las secretarías y dependencias que conforman la administración municipal, mediante el

cumplimiento de la normatividad establecida de Gobierno en Línea a través de la mejora continua, teniendo como pilares La CONFIDENCIALIDAD, DISPONIBILIDAD, INTEGRIDAD, NO REPUDIO Y AUTENTICIDAD de la información.

4. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El IMRDS con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de El IMRDS, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

- Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a El IMRDS
- Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con El IMRDS, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

- Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

OBJETIVOS

Preservar, proteger y administrar de forma eficiente la información de El IMRDS junto con los medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y controlada, enmarcada en el tratamiento de los riesgos de la información de El IMRDS, para

asegurar la sostenibilidad de El IMRDS y el nivel de eficacia.

ALCANCE

Esta política es de aplicación en el conjunto de Direcciones, oficinas y dependencias que componen El IMRDS, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la administración Pública a través de contratos o convenios con terceros y a todo el personal del IMRDS, independiente de su tipo de vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores que ejecute.

NIVEL DE CUMPLIMIENTO

a) El IMRDS ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, amparado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.
b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política. A continuación, se establecen los 12 principios de seguridad que soportan el MSPI de El IMRDS:

1. El IMRDS ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del Instituto, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de funcionarios provisionales, funcionarios con carrera administrativa, funcionarios con libre nombramiento y contratistas.
3. El IMRDS, protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos, incluyendo los datos personales conforme lo define la Ley 1581 de 2012 y las normas que complementen, definen o reglamentan.
4. El IMRDS, protegerá la información creada, procesada, transmitida o resguardada por sus procesos del instituto, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. El IMRDS, protegerá su información de las amenazas originadas por parte del personal.
6. El IMRDS, protegerá las instalaciones de procesamiento y la infraestructura

tecnológica que soporta sus procesos críticos.

7. El IMRDS, controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. El IMRDS, implementará control de acceso a la información, sistemas y recursos de red.
9. El IMRDS, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. El IMRDS, garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
11. El IMRDS, garantizará la disponibilidad de sus procesos del instituto y la continuidad de su operación basada en el impacto que pueden generar los eventos.
12. El IMRDS, garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

5. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1 Manual de políticas

El IMRDS con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la información en el IMRDS, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.
La seguridad de la información se entiende como la preservación de las siguientes características:

A. **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a el IMRDS.
B. **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
C. **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con el IMRDS, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

A. **Auditabilidad:** define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

B. **Protección a la duplicación:** consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
C. **No repudio:** se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
D. **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
E. **Confiabilidad de la Información:** es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

5.2 Objetivos

Preservar, proteger y administrar de forma eficiente la información del IMRDS junto con los medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y controlada, enmarcada en el tratamiento de los riesgos de la información del IMRDS, para asegurar la sostenibilidad del IMRDS y el nivel de eficacia.

5.3 Alcance

Esta política es de aplicación en el conjunto de Dirección, Subdirecciones, oficinas y dependencias que componen el IMRDS, a sus recursos, a la totalidad de los procesos internos o externos vinculados a la Administración Pública a través de contratos o convenios con terceros y a todo el personal del Instituto, independiente de su tipo de vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores que ejecute.

5.4 Nivel de Cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política. A continuación, se establecen los 12 principios de seguridad que soportan el MSPI del IMRDS:

1. El IMRDS ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades del Instituto, y a los requerimientos regulatorios

que le aplican a su naturaleza.

2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de funcionarios provisionales, funcionarios con carrera administrativa, funcionarios con libre nombramiento y contratistas.
3. El IMRDS, protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos, incluyendo los datos personales conforme lo define la Ley 1581 de 2012 y las normas que complementen, definen o reglamentan.
4. El IMRDS, protegerá la información creada, procesada, transmitida o resguardada por sus procesos del Instituto, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. El IMRDS, protegerá su información de las amenazas originadas por parte del personal.
6. El IMRDS, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. El IMRDS, controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. El IMRDS, implementará control de acceso a la información, sistemas y recursos de red.
9. El IMRDS, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. El IMRDS, garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
11. El IMRDS, garantizará la disponibilidad de sus procesos del Instituto y la continuidad de su operación basada en el impacto que pueden generar los eventos.
12. El IMRDS, garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

5.5 Normatividad Pertinente.

5.5.1 Normas que rigen para la estructura organizacional de seguridad de la información

Normas dirigidas a: EL DIRECTOR GENERAL

A. El DIRECTOR GENERAL debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

B. El DIRECTOR GENERAL debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.

C. El DIRECTOR GENERAL debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.

D. El DIRECTOR GENERAL debe promover activamente una cultura de seguridad de la información en el Instituto.

E. El DIRECTOR GENERAL debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la entidad y al personal provisto por terceras partes.

Normas dirigidas a: EL DIRECTOR GENERAL Y SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA

- El DIRECTOR GENERAL y la SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA, deben
  asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información del Instituto.

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

A. El Comité de Seguridad de la Información debe actualizar y presentar ante la Junta Directiva las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.

B. El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

C. El Comité de Seguridad de la Información debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

Normas dirigidas a: OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe liderar la generación de lineamientos para gestionar la seguridad de la información del IMRDS y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.

B. La Oficina De Gestión Tecnológica E Informática debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

C. La Oficina De Gestión Tecnológica E Informática debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica del IMRDS. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

A. La Oficina de Control Interno debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información del IMRDS a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.

B. La Oficina de Control Interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.

C. La Oficina de Control Interno debe informar a las áreas responsables los hallazgos de las auditorías.

Normas dirigidas a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes que realicen labores en o para el IMRDS, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

5.5.2 Normas para uso de dispositivos móviles

Normas dirigidas a: OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por el IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe establecer las configuraciones

aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por el IMRDS.

C. La Oficina De Gestión Tecnológica E Informática debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

D. La Oficina De Gestión Tecnológica E Informática debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.

E. La Oficina De Gestión Tecnológica E Informática debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

F. La Oficina De Gestión Tecnológica E Informática debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales del IMRDS; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.

G. La Oficina De Gestión Tecnológica E Informática debe instalar un software de antivirus tanto en los dispositivos móviles institucionales. como en los personales que hagan uso de los servicios provistos por el IMRDS.

H. La Oficina De Gestión Tecnológica E Informática debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

B. Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con

ellos al momento de su entrega.

C. Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

D. Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

E. Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

F. Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

G. Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

5.5.3 Normas para uso de conexiones remotas

Normas dirigidas a: OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática, deben analizar y aprobar los métodos de conexión remota a la plataforma tecnológica del IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica del IMRDS.

C. La Oficina De Gestión Tecnológica E Informática debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

D. La Oficina De Gestión Tecnológica E Informática debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica del IMRDS de manera permanente.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

- La Oficina de Control Interno debe, dentro de su autonomía, realizar auditorías sobre los controles implantados para las conexiones remotas a la plataforma tecnológica del IMRDS.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica del IMRDS y deben acatar las condiciones de uso establecidas para dichas conexiones.

B. Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores público, de hoteles o cafés internet, entre otros.

5.5.4 Normas relacionadas con la vinculación de funcionarios

Normas dirigidas a: SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA- GRUPO DE TALENTO HUMANO

A. El Grupo de Talento Humano debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en El IMRDS, antes de su vinculación definitiva.

B. El Grupo de Talento Humano debe certificar que los funcionarios del IMRDS firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

Normas dirigidas a: SUPERVISORES DE CONTRATO, SUBDIRECTORES.

- Cada Supervisor de Contrato y subdirector debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información del IMRDS.

Normas dirigidas a: PERSONAL PROVISTOS POR TERCERAS PARTES

A. El personal provisto por terceras partes que realicen labores en o para el IMRDS, deben firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

B. El personal provisto por terceras partes, deben garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad y aceptación de las Políticas de Seguridad de la Información del IMRDS.

5.5.5 Normas aplicables durante la vinculación de funcionarios y personal provisto por terceros

Normas dirigidas a: EL DIRECTOR GENERAL

A. El DIRECTOR GENERAL debe demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas, normas y demás lineamientos que desee establecer en el IMRDS.

B. El DIRECTOR GENERAL debe promover la importancia de la seguridad de la información entre los funcionarios del IMRDS y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.

C. El DIRECTOR GENERAL debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente del IMRDS, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Normas dirigidas a: OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe diseñar y ejecutar de manera permanente un programa de concienciación en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento el IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe capacitar y entrenar a los funcionarios del IMRDS en el programa de concienciación en seguridad de la información para evitar posibles riesgos de seguridad.

Normas dirigidas a: SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA

- La SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe aplicar el proceso disciplinario del IMRDS cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad de la información.

Normas dirigidas a: SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA - GRUPO DE

TALENTO HUMANO

- El Grupo de Talento Humano debe convocar a los funcionarios a las charlas y eventos programados como parte del programa de concienciación en seguridad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos, aplicando las sanciones pertinentes por la falta de asistencia no justificada.

Normas dirigidas a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes que por sus funciones hagan uso de la información del IMRDS, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

5.5.6 Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros

Normas dirigidas a: SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA - GRUPO DE TALENTO HUMANO

- El Grupo de Talento Humano debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios del IMRDS llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

Normas dirigidas a: SUPERVISORES DE CONTRATO, SUPERVISORES Y DIRECTORES

- Cada Supervisor de Contrato, subdirectores y Director debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios o personal provistos por terceras partes a La Oficina De Gestión Tecnológica E Informática.

Normas dirigidas a: OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

- La Oficina De Gestión Tecnológica E Informática debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe realizar la modificación o inhabilitación de usuarios.

5.5..7 Normas de responsabilidad por los activos de información

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

A. Los Subdirectores del IMRDS, deben actuar como propietarios de la información física y electrónica de la entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.

B. Los propietarios de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.

C. Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.

D. Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información del IMRDS, se encuentran sujetos a auditorías por parte de la Oficina de Control Interno y a revisiones de cumplimiento por parte de La Oficina De Gestión Tecnológica E Informática.

Normas dirigidas a: OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática es la propietaria de los activos de información correspondientes a la plataforma tecnológica del IMRDS y, en consecuencia, debe asegurar su apropiada operación y administración.

B. La Oficina De Gestión Tecnológica E Informática en conjunto con el Comité de Control de Cambios, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica del IMRDS.

C. La Oficina De Gestión Tecnológica E Informática debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

D. La Oficina De Gestión Tecnológica E Informática es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de las mismas a el IMRDS.

E. La Oficina De Gestión Tecnológica E Informática es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando les es formalmente solicitado.

F. La Oficina De Gestión Tecnológica E Informática debe realizar un análisis de riesgos de seguridad de manera periódica, sobre los procesos del IMRDS.

G. La Oficina De Gestión Tecnológica E Informática debe definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.

H. La Oficina De Gestión Tecnológica E Informática debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información del IMRDS.

Normas dirigidas a: LOS SUBDIRECTORES

A. Los Subdirectores, o quien ellos designen, deben autorizar a sus funcionarios el uso de los recursos tecnológicos, previamente preparados por La Oficina De Gestión Tecnológica E Informática.

B. Los Subdirectores, o quien ellos designen, deben recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiran del IMRDS o son trasladados de área.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los recursos tecnológicos del IMRDS, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen del IMRDS.

B. Los recursos tecnológicos del IMRDS provistos a funcionarios y personal suministrado por terceras partes, son proporcionados con el único fin de llevar a cabo las labores del Instituto; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

C. Los funcionarios no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.

D. Los funcionarios no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica del IMRDS.

E. Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

F. En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo a los Subdirectores y Director o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

5.5.8 Normas para la clasificación y manejo de la información

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- El Comité de Seguridad de la Información debe recomendar los niveles de clasificación de la información propuestos por La Oficina De Gestión Tecnológica E Informática y la guía de clasificación de la Información del IMRDS para que sean aprobados.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe definir los niveles de clasificación de la información para el IMRDS y, posteriormente generar la guía de clasificación de la Información.

B. La Oficina De Gestión Tecnológica E Informática debe socializar y divulgar la guía de clasificación de la Información a los funcionarios del IMRDS.

C. La Oficina De Gestión Tecnológica E Informática debe monitorear con una periodicidad establecida la aplicación de la guía de clasificación de la Información.

D. La Oficina De Gestión Tecnológica E Informática debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.

E. La Oficina De Gestión Tecnológica E Informática debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

F. La Oficina De Gestión Tecnológica E Informática deben definir los métodos de cifrado de la información de la Entidad de acuerdo al nivel de clasificación de los activos.

Normas dirigidas a: SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA– COORDINACIÓN DE ARCHIVO

A. La Coordinación de Archivo debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la

reconstrucción de la información del IMRDS, acogiéndose a procedimiento establecido para tal fin.

B. La Coordinación de Archivo debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.

C. La Coordinación de Archivo debe administrar el contrato de almacenamiento y resguardo de las cintas de Backup, otros medios de almacenamiento y documentos físicos del IMRDS con el proveedor del servicio.

D. La Coordinación de Archivo debe verificar el cumplimiento de los Acuerdos de Niveles de Servicio y Acuerdos de intercambio con el proveedor de custodia externo de los medios de almacenamiento y documentos del IMRDS.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

A. Los propietarios de los activos de información deben clasificar su información de acuerdo con las guías de clasificación de la Información establecida.

B. Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física del IMRDS.

B. La información física y digital del IMRDS debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

C. Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíes faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

D. Tanto los funcionarios como el personal provisto por terceras partes deben

asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

E. La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

5.5.9 Normas uso de periféricos y medios de almacenamiento

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática deben establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica del IMRDS.
B. La Oficina De Gestión Tecnológica E Informática debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica del IMRDS, de acuerdo con los lineamientos y condiciones establecidas.

C. La Oficina De Gestión Tecnológica E Informática debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento del IMRDS, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

D. La Oficina De Gestión Tecnológica E Informática debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica del IMRDS de acuerdo con el perfil del cargo del funcionario solicitante.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los funcionarios y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por La Oficina De Gestión Tecnológica E Informática.

B. Los funcionarios del IMRDS y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por La Oficina De Gestión Tecnológica E Informática.

C. Los funcionarios y personal provisto por terceras partes son responsables por la custodia de los medios de almacenamiento institucionales asignados.

D. Los funcionarios y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica del IMRDS.

5.5.10 Normas de acceso a redes y recursos de red

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red del IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe asegurar que las redes inalámbricas del IMRDS cuenten con métodos de autenticación que evite accesos no autorizados.

C. La Oficina De Gestión Tecnológica E Informática, debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red del IMRDS, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

D. La Oficina De Gestión Tecnológica E Informática debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red del IMRDS.

E. La Oficina De Gestión Tecnológica E Informática debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos del IMRDS, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

B. Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos del IMRDS deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

5.5.11 Normas de administración de acceso de usuarios

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información del IMRDS, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

B. La Oficina De Gestión Tecnológica E Informática, previa solicitud de los jefes inmediatos y/o Supervisores de los solicitantes de las cuentas de usuario y aprobación tanto de los propietarios de los sistemas de información, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.

C. La Oficina De Gestión Tecnológica E Informática, debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información del IMRDS; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

D. La Oficina De Gestión Tecnológica E Informática debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

E. La Oficina De Gestión Tecnológica E Informática debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

F. La Oficina De Gestión Tecnológica E Informática debe autorizar la creación o modificación de las cuentas de acceso de los recursos tecnológicos y sistemas de información del IMRDS.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

A. Es responsabilidad de los Propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con La Oficina De Gestión Tecnológica E Informática, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

B. Los propietarios de los activos de información deben verificar y ratificar

periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

Normas dirigidas a: LOS SUBDIRECTORES Y SUPERVISORES

- Los SUBDIRECTORES, Director Y Supervisores deben solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los funcionarios que laboran en sus áreas, acogiéndose al procedimiento establecidos para tal fin.

5.5.12 Normas de responsabilidades de acceso de los usuarios

Normas dirigidas a: TODOS LOS USUARIOS

A. Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información del IMRDS deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

B. Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.

C. Los funcionarios y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información del IMRDS deben acogerse a lineamientos para la configuración de contraseñas que estén implementados.

5.5.13 Normas de uso de altos privilegios y utilitarios de administración

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.

B. Oficina De Gestión Tecnológica E Informática debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.

C. La Oficina De Gestión Tecnológica E Informática debe verificar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción.

D. La Oficina De Gestión Tecnológica E Informática debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir

estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.

E. La Oficina De Gestión Tecnológica E Informática debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.

F. La Oficina De Gestión Tecnológica E Informática debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

G. La Oficina De Gestión Tecnológica E Informática, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica del IMRDS.

H. La Oficina De Gestión Tecnológica E Informática deben deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.

I. La Oficina De Gestión Tecnológica E Informática debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

J. La Oficina De Gestión Tecnológica E Informática debe validar que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los sistemas de información son aplicables a los usuarios administradores; así mismo, debe verificar que el cambio de contraseña de los usuarios administradores acoja el procedimiento definido para tal fin.

K. La Oficina De Gestión Tecnológica E Informática debe revisar periódicamente la actividad de los usuarios con altos privilegios en los registros de auditoría de la plataforma tecnológica y los sistemas de información.

5.5.14 Normas de control de acceso a sistemas y aplicativos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

A. Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

B. Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos del IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

C. La Oficina De Gestión Tecnológica E Informática debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

D. La Oficina De Gestión Tecnológica E Informática debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

E. La Oficina De Gestión Tecnológica E Informática debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

A. Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

B. Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.

C. Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

D. Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

E. Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

F. Los desarrolladores deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.

G. Los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.

H. Los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.

I. Los desarrolladores deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.

J. Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios

autorizados.

K. Los desarrolladores deben establecer que periódicamente se re-valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

5.5.15 Normas de controles criptográficos

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

B. La Oficina De Gestión Tecnológica E Informática debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.

C. La Oficina De Gestión Tecnológica E Informática debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.

D. La Oficina De Gestión Tecnológica E Informática, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

A. Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.

B. Los desarrolladores deben asegurarse que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la Dirección de Tecnología.

5.5.16 Normas de áreas seguras

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios de La Oficina De Gestión Tecnológica E Informática autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.

B. La Oficina De Gestión Tecnológica E Informática debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.

C. La Oficina De Gestión Tecnológica E Informática debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

D. La Oficina De Gestión Tecnológica E Informática debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

E. La Oficina De Gestión Tecnológica E Informática debe velar porque los recursos de la plataforma tecnológica del IMRDS ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

F. La Dirección de Tecnología debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

G. La Dirección de Tecnología debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: LOS SUBDIRECTORES, DIRECTORES Y SUPERVISORES

A. Los SUBDIRECTORES, Director y Supervisores que se encuentren en áreas restringidas deben velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en su áreas.

B. Los SUBDIRECTORES, Director y Supervisores que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.

C. Los SUBDIRECTORES, Director Y Supervisores deben velar porque las contraseñas

de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios del Instituto.

Normas dirigidas a: SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA

A. SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones del IMRDS.

B. SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones del IMRDS.

C. SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones del IMRDS.

D. SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.

E. SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe controlar el ingreso de los visitantes a los centros de cableado que están bajo su custodia.

F. SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe cerciorarse de que los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

G. SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA, con el acompañamiento de La Oficina De Gestión Tecnológica E Informática, debe verificar que el cableado se encuentra protegido con el fin de disminuir las intercepciones o daños.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los ingresos y egresos de personal a las instalaciones del IMRDS deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

B. Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones del IMRDS; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

C. Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

D. Los funcionarios del IMRDS y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

5.5.17 Normas de seguridad para los equipos institucionales

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones del IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica del IMRDS.

C. La Oficina De Gestión Tecnológica E Informática, en conjunto con la SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.

D. La Oficina De Gestión Tecnológica E Informática debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios del IMRDS y configurar dichos equipos acogiendo los estándares generados.

E. La Oficina De Gestión Tecnológica E Informática debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos del IMRDS y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

F. La Oficina De Gestión Tecnológica E Informática debe aislar los equipos de áreas sensibles, como la Dependencia de Hacienda para proteger su acceso de los demás funcionarios de la red de la empresa.

G. La Oficina De Gestión Tecnológica E Informática debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios del IMRDS, ya sea cuando son dados de baja o cambian de usuario.

H. La Oficina De Gestión Tecnológica E Informática debe evaluar y analizar los informes de verificación de equipos de cómputo de las diferentes áreas del IMRDS, en particular

de las áreas sensibles.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

- La Oficina de Control Interno tiene la responsabilidad de incluir dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo de todas las dependencias y puntos de atención de la entidad.

Normas dirigidas a: SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA

A. SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.

B. SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe restringir el acceso físico a los equipos de cómputo de áreas donde se procesa información sensible.

C. SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones del IMRDS cuente con la autorización documentada y aprobada previamente por La Oficina De Gestión Tecnológica E Informática.

D. SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera del IMRDS, posean pólizas de seguro.

Normas dirigidas a: TODOS LOS USUARIOS

A. La Oficina De Gestión Tecnológica E Informática es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos del IMRDS.

B. Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas de proporcione La Oficina De Gestión Tecnológica E Informática.

C. Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad del IMRDS el usuario responsable debe informar a la Plataforma de Mesa de Ayuda en donde se atenderá o escalará al interior de La Oficina De Gestión Tecnológica E Informática, con el fin de realizar una

asistencia adecuada. El usuario no debe intentar solucionar el problema.

D. La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos del IMRDS, solo puede ser realizado por los funcionarios de La Oficina De Gestión Tecnológica E Informática, o personal de terceras partes autorizado por dicha dirección.

E. Los funcionarios del IMRDS y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

F. Los funcionarios del IMRDS y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

G. Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

H. Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

I. Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

J. En caso de pérdida o robo de un equipo de cómputo del IMRDS, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

K. Los funcionarios del IMRDS y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

5.5.17 Normas de asignación de responsabilidades operativas

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

La Oficina De Gestión Tecnológica E Informática debe efectuar, a través de sus funcionarios, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica del IMRDS

A. Oficina De Gestión Tecnológica E Informática debe proporcionar a sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica del IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

C. La Oficina De Gestión Tecnológica E Informática, a través de sus funcionarios, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

D. La Oficina De Gestión Tecnológica E Informática debe emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica del IMRDS.

5.5.18 Normas de protección frente a software malicioso

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica del IMRDS y los servicios que se ejecutan en el IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

C. La Oficina De Gestión Tecnológica E Informática debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus,

incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

D. La Oficina De Gestión Tecnológica E Informática, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

E. La Oficina De Gestión Tecnológica E Informática, a través de sus funcionarios, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por La Oficina De Gestión Tecnológica E Informática; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

B. Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

C. Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

D. Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la plataforma de Mesa de Ayuda, para que, a través de ella, La Oficina De Gestión Tecnológica E Informática tome las medidas de control correspondientes.

5.5.19 Normas de copias de respaldo de la información

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

B. La Oficina De Gestión Tecnológica E Informática debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

C. La Oficina De Gestión Tecnológica E Informática, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

D. La Oficina De Gestión Tecnológica E Informática debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

E. La Oficina De Gestión Tecnológica E Informática debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información del IMRDS.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con La Oficina De Gestión Tecnológica E Informática, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Normas dirigidas a: TODOS LOS USUARIOS

- Es responsabilidad de los usuarios de la plataforma tecnológica del IMRDS identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

5.5.20 Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática, debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información del IMRDS.

B. La Oficina De Gestión Tecnológica E Informática, a través del Comité de revisión de

logs, deben definir de manera mensual cuáles monitoreos se realizarán de los registros de auditoría sobre los aplicativos donde se opera los procesos misionales del IMRDS. Así mismo, se deben reunir para analizar los resultados de cada monitoreo efectuado.

C. La Oficina De Gestión Tecnológica E Informática, a través de sus funcionarios, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.

D. La Oficina De Gestión Tecnológica E Informática debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información del IMRDS. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

Normas dirigidas a: OFICINA DE CONTROL INTERNO

A. La Oficina de Control Interno debe determinar los periodos de retención de los registros (logs) de auditoría de los recursos tecnológicos y los sistemas de información del IMRDS.

B. La Oficina de Control Interno debe revisar periódicamente los registros de auditoría de la plataforma tecnológica y los sistemas de información con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

A. Los desarrolladores deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.

B. Los desarrolladores deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por La Oficina De Gestión Tecnológica E Informática.

C. Los desarrolladores deben evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoría que brinden información adicional a la estrictamente requerida.

5.5.21 Normas de control al software operativo

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en el IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe asegurarse que el software operativo instalado en la plataforma tecnológica del IMRDS cuenta con soporte de los proveedores.

C. La Oficina De Gestión Tecnológica E Informática debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.

D. La Oficina De Gestión Tecnológica E Informática debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

E. La Oficina De Gestión Tecnológica E Informática debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo del IMRDS.

5.5.22 Normas para la gestión de vulnerabilidades

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las pruebas en el IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

C. La Oficina De Gestión Tecnológica E Informática debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.

D. La Oficina De Gestión Tecnológica E Informática, a través de sus funcionarios, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

E. La Oficina De Gestión Tecnológica E Informática, a través del Comité de vulnerabilidades, deben revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

5.5.23 Normas de gestión y aseguramiento de las redes de datos

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red del IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

C. La Oficina De Gestión Tecnológica E Informática debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para el IMRDS.

D. La Oficina De Gestión Tecnológica E Informática debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

E. La Oficina De Gestión Tecnológica E Informática debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica del IMRDS, acogiendo buenas prácticas de configuración segura.

F. La Oficina De Gestión Tecnológica E Informática, a través de sus funcionarios, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por el IMRDS en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

G. La Oficina De Gestión Tecnológica E Informática debe instalar protección entre las redes internas del IMRDS y cualquier red externa, que este fuera de la capacidad de control y administración del Instituto.

H. La Oficina De Gestión Tecnológica E Informática debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos del IMRDS.

5.5.24 Normas de uso del correo electrónico

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.

B. La Oficina De Gestión Tecnológica E Informática debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.

C. La Oficina De Gestión Tecnológica E Informática debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.

D. La Oficina De Gestión Tecnológica E Informática debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

E. La Oficina De Gestión Tecnológica E Informática, debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Normas dirigidas a: TODOS LOS USUARIOS

A. La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario del IMRDS o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.

B. Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional del IMRDS. El correo institucional no debe ser utilizado para actividades personales.

C. Los mensajes y la información contenida en los buzones de correo son propiedad del IMRDS y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

D. Los usuarios de correo electrónico institucional tienen prohibido él envió de cadenas

de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios del IMRDS y el personal provisto por terceras partes.

E. No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

F. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por el IMRDS y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

5.5.25 Normas de uso adecuado de internet

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

B. La Oficina De Gestión Tecnológica E Informática debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

C. La Oficina De Gestión Tecnológica E Informática debe monitorear continuamente el canal o canales del servicio de Internet.

D. La Oficina De Gestión Tecnológica E Informática debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

E. La Oficina De Gestión Tecnológica E Informática debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

F. La Oficina De Gestión Tecnológica E Informática debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los usuarios del servicio de Internet del IMRDS deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

B. Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

C. No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, web proxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

D. Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, MSN, Yahoo, Sype, Net2phone, y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio del IMRDS.

E. No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y La Oficina De Gestión Tecnológica E Informática, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

F. No está permitido el intercambio no autorizado de información de propiedad del IMRDS, de sus clientes y/o de sus funcionarios, con terceros.

5.5.26 Normas de intercambio de información

Normas dirigidas a: ORDENADORES DE GASTOS

A. Ordenadores De Gastos, en acompañamiento con La Oficina De Gestión Tecnológica E Informática, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre el instituto y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de

dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por el IMRDS a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.

B. Ordenadores De Gastos debe establecer en los contratos que se establezcan con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios del IMRDS que les ha sido entregada en razón del cumplimiento de los objetivos misionales del IMRDS.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

A. Los propietarios de los activos de información deben velar porque la información del IMRDS o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

B. Los propietarios de los activos de información deben asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregada a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.

C. Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor del IMRDS y la fecha de entrega/recepción.

D. Los propietarios de los activos de información deben autorizar los requerimientos de solicitud/envío de información del IMRDS por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.

E. Los propietarios de los activos de información deben asegurarse que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales del IMRDS, así como del procedimiento de intercambio de información.

F. Los propietarios de los activos de información deben verificar la destrucción de la información suministrada a los terceros, realizada por ellos una vez esta ha cumplido el cometido por el cual fue enviada.

Normas dirigidas a: CORRESPONDENCIA

A. La Correspondencia de cada dependencia debe acoger el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.

B. La Correspondencia de cada de dependencia debe certificar que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por el IMRDS, y que estos permitan ejecutar rastreo de las entregas.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información,

   permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

B. La Oficina De Gestión Tecnológica E Informática debe definir y establecer el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación del IMRDS, reciben o envían información de los beneficiarios del IMRDS, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad del IMRDS.

C. La Oficina De Gestión Tecnológica E Informática debe velar porque el intercambio de información del IMRDS con entidades externas se realice en cumplimiento de las Políticas de seguridad para el intercambio de información aquí descritas, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.

D. La Oficina De Gestión Tecnológica E Informática debe autorizar el establecimiento del vínculo de transmisión de información con terceras partes, para que posteriormente las áreas funcionales realicen las actividades de transmisión requeridas en cada caso.

Normas dirigidas a: TERCEROS CON QUIENES SE INTERCAMBIA INFORMACIÓN DEL IMRDS

A. Los terceros con quienes se intercambia información del IMRDS deben darle manejo

adecuado a la información recibida, en cumplimiento de las Políticas de seguridad del IMRDS, de las condiciones contractuales establecidas y del Procedimiento de intercambio de información.

B. Los terceros con quienes se intercambia información del IMRDS deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

Normas dirigidas a: TODOS LOS USUARIOS:

A. Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible del IMRDS o de sus beneficiarios.

B. No está permitido el intercambio de información sensible del IMRDS por vía telefónica.

5.5.27 Normas para el establecimiento de requisitos de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN Y LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro del IMRDS formalmente asignada.

B. La Oficina De Gestión Tecnológica E Informática debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas

prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

C. Las áreas propietarias de los sistemas de información, en acompañamiento con La Oficina De Gestión Tecnológica E Informática deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

D. Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

E. La Oficina De Gestión Tecnológica E Informática debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de

autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

A. Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

B. Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.

C. Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.

D. Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

E. Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.

F. Los desarrolladores deben utilizar usar los protocolos sugeridos por La Oficina De Gestión Tecnológica E Informática en los aplicativos desarrollados.

G. Los desarrolladores deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

5.5.28 Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas

Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN

A. Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

B. Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

B. La Oficina De Gestión Tecnológica E Informática debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del IMRDS.

C. La Oficina De Gestión Tecnológica E Informática debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

D. La Oficina De Gestión Tecnológica E Informática debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

E. La Oficina De Gestión Tecnológica E Informática, a través de sus funcionarios, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

F. La Oficina De Gestión Tecnológica E Informática debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información del IMRDS.

G. La Oficina De Gestión Tecnológica E Informática debe verificar que las pruebas de seguridad sobre los sistemas de información se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

A. Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y

lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

B. Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo del IMRDS; dicho soporte debe contemplar tiempos de respuesta aceptables.

C. Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

D. Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

E. Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

F. Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.

G. Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.

H. Los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

I. Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

J. Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

K. Los desarrolladores deben remover información innecesaria en los encabezados de

respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

L. Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.

M. Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.

N. Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

O. Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

P. Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

5.5.29 Normas para la protección de los datos de prueba

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.

B. La Oficina De Gestión Tecnológica E Informática debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

5.5.30 Normas de inclusión de condiciones de seguridad en la relación con terceras partes

Normas dirigidas a: GRUPO ASESORA JURÍDICA Y LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. El grupo Asesora Jurídica y La Oficina De Gestión Tecnológica E Informática deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que

adquieran o supervisen recursos y/o servicios tecnológicos.

B. El grupo Asesora Jurídica y La Oficina De Gestión Tecnológica E Informática deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe establecer las condiciones de conexión

adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos del IMRDS.

B. La Oficina De Gestión Tecnológica E Informática debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

C. La Oficina De Gestión Tecnológica E Informática debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica del IMRDS.

D. La Oficina De Gestión Tecnológica E Informática debe evaluar y aprobar los accesos a la información del IMRDS requeridos por terceras partes.

E. La Oficina De Gestión Tecnológica E Informática debe identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.

Normas dirigidas a: SUPERVISORES DE CONTRATOS CON TERCEROS

- Los Supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información del IMRDS a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento del IMRDS, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

5.5.31 Normas de gestión de la prestación de servicios de terceras partes

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos del IMRDS.

B. La Oficina De Gestión Tecnológica E Informática deben verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA Y SUPERVISORES DE CONTRATOS CON TERCEROS

A. La Oficina De Gestión Tecnológica E Informática y los Supervisores de contratos con terceros deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.

B. Los Supervisores de contratos con terceros, con el apoyo de La Oficina De Gestión Tecnológica E Informática, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

5.5.32 Normas para el reporte y tratamiento de incidentes de seguridad

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los activos de información deben informar a La Oficina De Gestión Tecnológica E Informática, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

B. La Oficina De Gestión Tecnológica E Informática debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad de la Información aquellos en los que se considere pertinente.

C. La Oficina De Gestión Tecnológica E Informática debe designar personal calificado,

para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re-ocurrencia.

D. La Oficina De Gestión Tecnológica E Informática y la Secretaría General, crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Normas dirigidas a: TODOS LOS USUARIOS

A. Es responsabilidad de los funcionarios del IMRDS y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

B. En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios deben notificarlo a La Oficina De Gestión Tecnológica E Informática para que se registre y se le dé el trámite necesario.

5.5.33 Normas de redundancia

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática deben analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para el IMRDS y la plataforma tecnológica que los apoya.

B. La Oficina De Gestión Tecnológica E Informática y debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos del IMRDS.

C. La Oficina De Gestión Tecnológica E Informática, a través de sus funcionarios, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad del IMRDS.

5.5.34 Normas de cumplimiento con requisitos legales y contractuales

Normas dirigidas a: GRUPO ASESOR JURÍDICO Y LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

- El grupo Asesor Jurídico y La Oficina De Gestión Tecnológica E Informática deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a el IMRDS y relacionados con seguridad de la información.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe certificar que todo el software que se ejecuta en el IMRDS esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

B. La Oficina De Gestión Tecnológica E Informática debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles del IMRDS para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo corresponda únicamente al permitido.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.

B. Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

5.5.35 Normas de privacidad y protección de datos personales

Normas dirigidas a: ÁREAS QUE PROCESAN DATOS PERSONALES

A. Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades del IMRDS.

B. Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

C. Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

D. Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

E. Las áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Gestión Tecnológica E Informática debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros del IMRDS de los cuales reciba y administre información.

B. La Oficina De Gestión Tecnológica E Informática debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información del IMRDS o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.
B. Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

5.6 RESPONSABILIDADES

Todos los subdirectores, Director General o equivalentes, titulares de Unidades Organizativas, tanto se trate de autoridades políticas o personal técnico y sea cual fuere su nivel jerárquico son responsables de la implementación de esta Política de Seguridad de la

Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal del IMRDS, cualquiera sea su situación de vinculación, el área a la cual se encuentre asignado y cualquiera sea el nivel de las tareas que desempeñe.

Las máximas autoridades del IMRDS aprueban esta Política y son responsables de la autorización de sus modificaciones.

El **Comité de Seguridad de la Información** del IMRDS, procederá a revisar y proponer a la máxima autoridad del Instituto para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información; garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la seguridad de la información dentro del IMRDS y coordinar el proceso de administración de la continuidad de las actividades del Instituto.

El **Coordinador del Comité de Seguridad de la Información** será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

El **responsable de Seguridad Informática** cumplirá funciones relativas a la seguridad de los sistemas de información del IMRDS, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.

Los **Propietarios de la Información** son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad del IMRDS, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El **responsable del Área de Recursos Humanos** o quién desempeñe esas funciones, cumplirá la

función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la

implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continuada en materia de seguridad.

El **responsable del Área Informática cumplirá** la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología del IMRDS. Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

El **responsable del Área Legal** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación del IMRDS con sus empleados y con terceros. Asimismo, asesorará en materia legal a el IMRDS, en lo que se refiere a la seguridad de la información.

Los **usuarios de la información y de los sistemas** utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

La **Unidad de Control Interno**, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

6 PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

6.1 Procedimiento de asignación de equipos y acceso a Sistemas de Información

El IMRDS pondrá a disposición de sus funcionarios y colaboradores todas aquellas herramientas y recursos tecnológicos necesarios, en la medida de sus posibilidades, para realizar sus respectivas funciones en el Instituto.

En este sentido, el primer hito corresponde a la asignación de equipos computacionales y la creación de cuentas de acceso a la red del IMRDS. Posteriormente, al usuario se le proporcionan permisos para acceder a los distintos Sistemas de Información que maneja el IMRDS, los cuales corresponden a software diseñados, con el objetivo de facilitar las funciones establecidas para el IMRDS y apoyar la toma de decisiones de las distintas áreas que la conforman. En tanto, todo funcionario o contratista deberá devolver los activos pertenecientes a el Instituto, como consecuencia de la finalización de su relación laboral con el IMRDS, momento en el cual se deben cerrar todas sus cuentas asociadas a la red interna.

6.2 Objetivo General

Establecer las actividades necesarias para la asignación de equipos y creación de cuentas de acceso

a los Sistemas de Información del IMRDS, así como también para la devolución de activos y cierre de las cuentas.

6.3 Alcance

Este procedimiento aplica a todos los funcionarios (provisional, carrera administrativa y libre nombramiento), contratistas, terceros que presten servicios a el IMRDS y alumnos en práctica o que realicen algún otro tipo de actividad académica, para lo cual requieran el uso de sistemas y servicios basados en tecnologías de información.

6.4 Responsabilidades

Para cumplir los objetivos del presente procedimiento, se establecen los siguientes roles y responsabilidades

6.4.1 La Dependencias del IMRDS

- A las Dependencias les corresponderán las siguientes responsabilidades:
- Notificar a Recursos Humanos, sobre las vinculaciones y desvinculaciones del personal de cada dependencia, con la debida antelación para que sea factible realizar las actividades descritas en este procedimiento.
- Solicitar el acceso a Sistemas de Información para el personal de su dependencia, a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA.
- Administrar el uso de los Sistemas de Información relacionados con el IMRDS.
- Capacitar a su personal en el uso de los Sistemas de Información relacionados con el IMRDS

6.4.2 Recursos Humanos

Es responsable de notificar de forma consolidada a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, sobre las vinculaciones y desvinculaciones del personal de cada área del IMRDS, con la debida antelación para que sea factible realizar las actividades descritas en este procedimiento.

6.4.3 Subdirección Administrativa Y Financiera

Es responsable de mantener actualizado el inventario de activos fijos del IMRDS, el cual incluye equipos informáticos.

6.4.4 La oficina de gestión tecnológica e informática

Corresponderá a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA las siguientes responsabilidades:

Velar por el cumplimiento de este procedimiento y de los tres principios básicos de la Seguridad de la Información, de la siguiente forma:

- Integridad: tomar resguardos e implementar herramientas para que la información se mantenga completa, actualizada y veraz, sin modificaciones inapropiadas o corruptas.

- Confidencialidad: tomar resguardos e implementar herramientas para que la información esté protegida de personas/usuarios no autorizados.

- Disponibilidad: tomar resguardos e implementar herramientas para que todos los usuarios autorizados puedan acceder a los Sistemas de Información cuando lo requieran, con objeto de desempeñar sus funciones.

Responder a las notificaciones enviadas por recursos humanos, sobre vinculaciones y desvinculaciones de funcionarios o colaboradores de cada dependencia del IMRDS, a través de las acciones indicadas en la sección 1.5 y en el procedimiento de seguridad de redes.

Proporcionar la información que requiera SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA, con objeto de mantener actualizado el inventario de activos fijos, respecto a equipos informáticos.

Mantener actualizado los siguientes registros:

- Inventario de los activos informáticos (licencias y equipos), incluyendo los asignados a usuarios y aquellos en almacén, junto a los formularios de asignación y devolución de equipos.

- Notificaciones enviadas por recursos humanos, sobre vinculaciones y desvinculaciones de funcionarios o colaboradores de cada área del IMRDS.

- Usuarios activos y no activos en la red IMRDS.

- Usuarios con permisos para acceder a cada sistema de información.

6.4.5. Usuarios de Sistemas de Información

Todos los usuarios de los Sistemas de Información que maneja el IMRDS, ya sean a planta o contratistas deben regirse bajo lo establecido en este procedimiento.

En particular, los usuarios deben velar por el cumplimiento de los tres principios básicos de la Seguridad de la Información, de la siguiente forma:

- Integridad: La información que registra o consulta desde los distintos Sistemas debe mantenerse completa, actualizada y veraz, sin modificaciones inapropiadas o corruptas.
- Confidencialidad: La información que registra o consulta desde los distintos Sistemas debe estar protegida de personas/usuarios no autorizados.
- Disponibilidad: Los equipos computacionales proporcionados para desempeñar sus funciones deben ser utilizados de forma apropiada, con objeto de contribuir a la disponibilidad de los servicios informáticos del IMRDS. Además, en caso de que un Sistema de Información presente problemas deberá ceñirse a lo establecido en el "Procedimiento de desarrollo y actualización de Sistemas de Información".

6.5 Descripción del Procedimiento

6.5.1 Inventario de activo fijo tecnológico

Se requiere mantener un registro de los activos fijos tecnológicos, durante todas las etapas correspondientes (adquisición, almacenamiento en almacén y asignación). Para esto, se deben cumplir los siguientes pasos:

Una vez que el activo fijo es recibido, LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA deberá actualizar su registro de activos con los siguientes datos: número de licitación asociado, período de garantía, descripción del producto (modelo, marca, etc.), número de serie, entre otros.

Posteriormente, LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA deberá informar a Oficina de Asesora Jurídica sobre la recepción del producto y proporcionar la información base indicada en el párrafo anterior. De este modo, almacén que pertenece a la SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA lo incluirá en el inventario de activos fijos del IMRDS y le asignará un código correlativo, el cual será informado al personal del LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA.

Si un equipo es asignado a un usuario, será responsabilidad del LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA registrar la información relevante a la asignación, incluyendo nombre del usuario, fecha de asignación, Dependencia y oficina de desempeño, entre otros, lo cual deberá ser informado a Almacén, con objeto de mantener actualizado el inventario institucional de activos fijos.

Si hubiera insumos computacionales defectuosos, susceptibles de ser dados de baja, LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA se entrega a almacén, con objeto de gestionar el acto administrativo correspondiente.

Al menos una vez en el semestre, el Encargado de Infraestructura y Redes de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA y lo quienes ellos designen, se reunirán para cruzar y validar la información de activo fijo tecnológico, quedando esto reflejado en un acta de reunión con los compromisos adquiridos, si es que los hubiera.

6.5.2 Asignación de equipos y creación de cuentas

La asignación de equipos informáticos y la creación de cuentas para acceder a la red IMRDS son actividades que realizará LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, de acuerdo a las notificaciones consolidadas que enviará la Sección de Desarrollo de las Personas. Es responsabilidad de cada dependencia del IMRDS informar con la debida antelación a Recursos Humanos, para que ésta pueda recopilar todos los antecedentes necesarios y luego notifique al LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, el cual deberá proceder con las acciones indicadas a continuación:

Habilitar estaciones de trabajo de nuevos funcionarios o colaboradores, con respecto a aspectos de tecnologías de información, configurando los equipos que correspondan (computador, teléfono, etc.). Al momento de recibir los equipos o insumos computacionales (incluyendo cambios), el usuario deberá firmar el formulario de asignación de activos, que proporcionará LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA.

Crear credenciales de acceso (usuario y contraseña) en el servicio de directorio para acceder a la red IMRDS y al correo electrónico institucional, de acuerdo a lo establecido en el procedimiento de seguridad de redes.

Actualizar los registros indicados en la sección 1.5.1, particularmente, en relación con la asignación de equipos.

6.5.3 Acceso a sistemas de información

La solicitud de acceso específico a sistemas de información para nuevos funcionarios o colaboradores, deberá ser gestionada por cada dependencia del IMRDS a través de sus SUBDIRECTORES o quiénes estos designen para tal función.

La solicitud de acceso deberá ser realizada a través del correo electrónico. Cabe destacar que esta función estará disponible solo para las personas autorizadas por las SUBDIRECTORES o supervisores de cada Dependencia, lo cual debe ser formalizado a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA. En la solicitud de acceso se deberá indicar:

Usuario que requiere permisos de acceso.

Detallar el o los sistemas a los cuales el usuario deberá tener acceso.

Detalle del perfil de usuario con el que debe contar el funcionario para cada uno de los sistemas a los cuales se solicita acceso.

6.5.4 Devolución de activos y des habilitación de cuentas

La recuperación de activos y la des habilitación de cuentas para acceder a la red IMRDS son actividades que realizará LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, de acuerdo a las notificaciones consolidadas que enviará recursos humanos. Es responsabilidad de cada dependencia del IMRDS informar con la debida antelación a recursos humanos, para que ésta pueda recopilar todos los antecedentes necesarios y luego notifique a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, el cual deberá proceder con las acciones indicadas a continuación:

Recuperar los activos asignados al usuario desvinculado. Al momento de devolver los equipos tecnológicos, el usuario deberá firmar el formulario de devolución de activos, que proporcionará LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA. En caso de que el usuario no se encuentre al momento de retirar los equipos, el formulario deberá ser firmado por el supervisor del contrato o por el director del equipo de trabajo del usuario.

Deshabilitar las credenciales de acceso (usuario y contraseña) en el Servicio de Directorio Institucional, con el objeto de impedir el acceso a la red IMRDS y al correo electrónico institucional.

Respaldar la información del computador del usuario desvinculado, de acuerdo a lo establecido en el procedimiento de respaldo de información.

Actualizar los registros indicados en la sección 1.5.1, que correspondan.

Informar a los supervisores, en caso de que no se devuelvan todos los equipos tecnológicos asignados o sean devueltos con desperfectos, para que se tomen las medidas que correspondan.

6.6 Instructivos y Procedimientos

6.6.1 Instructivo de uso de computadores personales

Dentro de los recursos tecnológicos asignados, se consideran los equipos de computación y periféricos, ya sean portátiles o fijos (de sobremesa), los cuales son herramientas de trabajo pertenecientes a el IMRDS. De este modo, los equipos serán asignados al personal para darle un uso institucional y serán configurados, de acuerdo a los lineamientos establecidos para tales fines.

A continuación, se detallan las condiciones para el uso de computadores por parte de los usuarios:

- El uso del computador asignado será de carácter estrictamente institucional.
- El usuario tiene como obligación respetar los deberes y restricciones que establezca la institución.
- El usuario sólo podrá utilizar el equipo con las aplicaciones requeridas para realizar sus funciones, si requiere una nueva aplicación o eliminar una existente, deberá contactar al personal del Departamento de Gestión de la Información, generando un ticket en la plataforma web http:/172.16.0.94, llamando a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA o correo electrónico, informando de esto a su supervisor y/o jefatura directa.
- Está estrictamente prohibido el uso de software comercial no licenciado en los equipos institucionales.
- Los computadores asignados al personal serán propiedad del IMRDS y no del usuario; y por tanto se le deberá dar un uso estrictamente institucional.
- El uso de internet debe ser exclusivamente para los temas de trabajo, con objeto de no saturar la red del IMRDS.
- Aquellos usuarios que manejen activos de información de carácter confidencial en sus equipos asignados deberán tomar los resguardos necesarios para que dicha información no sea filtrada a terceros en caso de pérdida del equipo. Si necesitan apoyo para realizar un resguardo adecuado, deben tomar contacto con personal de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, generando un ticket en la plataforma web http:/172.16.0.94, llamando a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA o correo electrónico.
- Los equipos portátiles se deberán dejar en el escritorio con sujetadores antirrobo provistos por la institución. Si no posee uno, debe dar aviso al personal de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA generando un ticket en la plataforma web http:/172.16.0.94, llamando a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA o correo electrónico.
- Será responsabilidad del funcionario del IMRDS solicitar mantención de sus computadores asignados por LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, generando un ticket en la plataforma web http:/172.16.0.94, llamando a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA o correo electrónico.
- No está permitido modificar o instalar componentes a los equipos sin asistencia y autorización por LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA.
- Es responsabilidad del usuario mantener un respaldo de su información. De todos modos, con objeto de almacenar la información más relevante y sensible se disponen carpetas compartidas en la red del IMRDS, asignadas para cada División, Departamento, u Oficina, en el servidor de archivos, las cuales se respaldan periódicamente para evitar perdida de información. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA pueden asistir en esta labor, para lo cual se

requiere generar un ticket en la plataforma web http:/172.16.0.94, llamando a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA o correo electrónico.

- No está permitido almacenar información de carácter personal en los equipos institucionales.
- En caso de requerir equipos portátiles o proyectores para el desarrollo de reuniones, talleres u otras actividades, deberán ser solicitados a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, generando un ticket a través de la plataforma web http:/172.16.0.94, llamando a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA o correo electrónico.
- Se podrán retirar equipos informáticos desde las dependencias del IMRDS, solo para actividades institucionales. Para ello se requerirá autorización de la jefatura correspondiente y cumplir con lo indicado en el punto anterior, cuando corresponda. En caso de daño y/o pérdida de equipos retirados de las dependencias del IMRDS, se realizará una investigación, que podría derivar en sanciones administrativas.

6.6.2 Procedimiento de desarrollo y actualización de Sistemas de Información

6.6.2.1 Introducción

Los sistemas de información corresponden a software diseñados, con el objetivo de facilitar las funciones establecidas para IMRDS y apoyar la toma de decisiones de las distintas dependencias que la conforman.

Es necesario destacar que, en su conjunto, estos sistemas constituyen la plataforma electrónica del IMRDS, la cual debe sustentar los siguientes usos:

Permitir la adecuada administración de los Sistemas del IMRDS.

Permitir la aplicación útil para la detección temprana de desviaciones o irregularidades y la consecuente adopción oportuna de las medidas o acciones que correspondan.

Mantener un historial sistematizado y actualizado de las acciones de fiscalización realizadas respecto de cada sujeto fiscalizado y sus resultados, así como de los procesos sancionatorios de que sean objeto y sus resultados

Permitir obtener información útil para la priorización de futuras fiscalizaciones y para la resolución de futuros procedimientos sancionatorios.

De este modo, existe una necesidad de desarrollar sistemas para sistematizar información. Por otro lado, durante su vida útil los Sistemas de Información se enfrentan a la organización y sus condiciones, las cuales pueden presentar variaciones. Por lo tanto, para que tales sistemas respondan a los requisitos operativos para los que fueron desarrollados inicialmente y, además, se adapten a las nuevas condiciones, en algunas ocasiones se necesitarán ajustes menores, mientras que en otras situaciones se requerirán de renovaciones completas.

Este documento detalla el procedimiento tanto para el desarrollo de nuevos sistemas de información, como para enfrentar cambios de manera ordenada y sistematizada, en busca de un mejor resultado para las partes interesadas.

6.6.2.2 Objetivo General

Establecer las directrices para regular tanto la creación, como la implementación de cambios, con relación a Sistemas de Información que dependan de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA del IMRDS.

6.6.2.3 Alcance

Este procedimiento considera los Sistemas de Información que están bajo la administración del LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA del IMRDS y es aplicable a todos los funcionarios (planta, contratistas) y terceros que presten servicios a el IMRDS.

6.6.2.4 Responsabilidades

Para cumplir los objetivos del presente procedimiento, se establecen los siguientes roles y responsabilidades.

6.6.2.5 Las Dependencias del IMRDS

Les corresponderán las siguientes responsabilidades:

- Velar por el cumplimiento de este procedimiento.
- Designar una contraparte oficial para cada proyecto.
- Contribuir al cumplimiento de los plazos establecidos para cada proyecto.
- Administrar el uso de los Sistemas de Información relacionados con el instituto.
- Capacitar a su personal en el uso de los Sistemas de Información relacionados con el instituto.

6.6.2.6 LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

Le corresponderán las siguientes responsabilidades:

- Velar por el cumplimiento de este procedimiento y de los tres principios básicos de la Seguridad de la Información, de la siguiente forma:
    - Integridad: tomar resguardos e implementar herramientas para que la información se mantenga completa, actualizada y veraz, sin modificaciones inapropiadas o corruptas.
    - Confidencialidad: tomar resguardos e implementar herramientas para que la información esté protegida de personas/usuarios no autorizados.
    - Disponibilidad: tomar resguardos e implementar herramientas para que todos los usuarios autorizados puedan acceder a los Sistemas de Información cuando lo requieran, con objeto de desempeñar sus funciones.

- Mantener un inventario de los Sistemas de Información, que permita llevar un control de sus versiones.
- Mantener expedientes con la documentación indicada en la sección 2.5 y las auditorías realizadas para cada proyecto.
- Velar por la integración de los distintos Sistemas de Información del IMRDS, cuando corresponda.
- Administrar las bases de datos asociados a los Sistemas de Información del IMRDS.
- Implementar controles de seguridad para los sistemas que interoperen o intercambien datos, con otros sistemas o base de datos, pertenecientes a el IMRDS u otros Organismos del Estado.
- Capacitar a los usuarios ante el lanzamiento de nuevos desarrollos o la implementación de cambios relevantes de sistemas de información, de forma previa al paso a producción, idealmente.
- Planificar, coordinar e implementar actualizaciones de los sistemas operativos y otras las licencias que soportan a los Sistemas de Información, cuando corresponda.
- Exigir la aplicación de este procedimiento a los desarrollos efectuados por personal externo.

6.6.2.6 Roles específicos

Para el desarrollo y actualización de sistemas de información se identifican los siguientes roles específicos:

- Encargado de Sección de Desarrollo y Mantención de Sistemas de Información en LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA: es el responsable de coordinar actividades y proyectos de la sección.
- Coordinador de proyectos en LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA: es el encargado de orientar y apoyar al Ingeniero responsable del proyecto, velando por la incorporación de los procesos de negocios y la integración de sistemas afines.

- Ingeniero responsable del proyecto en LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA: es el encargado de implementar el proyecto en sus distintas etapas (especificación de requerimientos, codificación, pruebas, paso a producción, entre otros) y mantener actualizada la ficha y la documentación del proyecto.
- Administrador de las bases de datos en LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA: es el responsable de validar y dar conformidad a la base de datos que será puesta en producción, velando por la integración de las distintas bases de datos que, en conjunto, constituyen la plataforma electrónica del IMRDS. También debe asistir en la ejecución de cambios en ambiente de producción.
- Ingeniero de la Sección de Análisis e Inteligencia de Negocios en LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA: es el responsable de asistir al equipo de desarrollo del LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, bajo la lógica de la explotación y análisis de los datos contenidos en un sistema de información.
- Contraparte de la dependencia: es el designado por la dependencia solicitante o beneficiaria de un proyecto para asistir al equipo de desarrollo del LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, en todas sus etapas, incluyendo actividades como: especificar el requerimiento, explicar los flujos de negocios, realizar pruebas, entre otras.

6.6.2.7. Desarrollo de nuevos Sistemas de Información

El desarrollo de nuevos Sistemas de Información deberá considerar las siguientes etapas:

Solicitud de Requerimientos

Esta etapa tiene por objetivo identificar las necesidades de nuevos desarrollos y priorizarlas, en función de los intereses institucionales. Para ello, se consideran las siguientes actividades:

- LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA comunicará a las dependencias del IMRDS los períodos de recepción de propuestas de nuevos desarrollos, vía oficio, con la antelación necesaria para que las áreas puedan recopilar los antecedentes y preparar los requerimientos. En particular, se debe considerar, al menos, un período de recepción de propuestas por año, con objeto de planificar los recursos y las actividades necesarias para implementar los proyectos seleccionados.
- Las dependencias deberán enviar sus requerimientos a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA de forma consolidada, vía oficio. Se deberá completar un formulario de requerimiento por cada nuevo desarrollo que sea solicitado, de acuerdo al formato que LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA establezca para estos fines. En particular, la dependencia solicitante deberá indicar: contraparte designada, descripción del requerimiento, alcance (procesos involucrados y relación con otros Sistemas de Información), impactos y plazos asociados, entre otros. No se abordarán solicitudes remitidas fuera de los

plazos establecidos, salvo expresa orden de SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA.

- Los requerimientos recibidos serán analizados por LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA. El resultado de este análisis corresponderá a un informe consolidado sobre la factibilidad técnica y la disponibilidad de recursos para implementar los requerimientos.
- El informe consolidado preparado por LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA será remitido a SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA, quien
  resolverá y priorizará los desarrollos que serán atendidos, definiendo los recursos asociados.
- Posteriormente, se informará a las dependencias del IMRDS sobre los resultados finales del proceso de priorización.

Especificación de Requerimientos

Esta etapa tiene por objetivo especificar elementos o detalles de un proyecto aprobado para su desarrollo, de modo de disminuir las incertidumbres asociadas y dimensionar los recursos necesarios.

Requiere de un trabajo conjunto entre personal de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA y la contraparte de la dependencia solicitante, quien deberá proporcionar todos los insumos necesarios para especificar la solicitud original, de modo de facilitar la comprensión del proyecto por parte del equipo de desarrollo de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, idealmente a través de un documento consolidado.

El resultado final de esta etapa corresponderá a un informe que elaborará LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA y que deberá ser firmado por ambas partes. Los elementos a considerar en esta etapa son los siguientes:

- Diagramas de flujos de procesos.
- Casos de usos (identificación de perfiles de usuarios).
- Requerimientos funcionales (servicios o funciones que debe proporcionar el sistema).
- Requerimientos no funcionales (restricciones delosservicios o funciones ofrecidos por el sistema).
- Cronograma referencial de actividades.

Plan de proyecto

Esta etapa tiene por objetivo establecer los responsables del desarrollo de un proyecto aprobado, junto al cronograma de actividades y a aspectos específicos, adicionales a los abordados en la etapa anterior. Requiere de un trabajo conjunto entre personal de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA y la contraparte de la dependencia solicitante. El resultado final de esta etapa corresponderá a un informe que

elaborará LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA y que deberá ser firmado por ambas partes. Este informe deberá ser reportado a la SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA, para su aprobación. Los elementos a considerar para la confección del plan de proyecto son los siguientes:

- Equipo de trabajo.
- Arquitectura del sistema.
- Propuesta del modelo de datos del sistema.
- Maquetas de interfaz de usuario.
- Módulos del sistema (entrega de productos por etapas).
- Cronograma de actividades definitivo.
- Conjunto de pruebas.
- Riesgos involucrados.
- Criterios de aceptación.
- En el caso de desarrollar una nueva versión de un sistema, se deberá considerar la realización de un plan de migración de datos.

Construcción

Esta etapa considera la implementación de un proyecto aprobado (codificación), de acuerdo a las condiciones establecidas en las etapas anteriores, generando como resultado un producto preliminar, disponible para la etapa de pruebas. La gestión del código fuente y de las bases de datos deberá regirse según lo establecido en este procedimiento y en las directrices que establezca el IMRDS para tales fines.

Pruebas

Esta etapa considera realizar pruebas sobre el producto de la etapa anterior, de acuerdo a las condiciones establecidas para el proyecto, con el objetivo de verificar su calidad en base a la identificación de posibles fallas o errores de programación, usabilidad, programación, etc. Se deberán considerar pruebas del personal de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA que no hayan participado directamente en el desarrollo y, posteriormente, pruebas de los usuarios finales del producto. Las revisiones deberán quedar documentadas, según tipo de problema detectado, junto a la solución implementada.

Las pruebas funcionales tienen como fin validar que el sistema de información cumple con los requisitos básicos de funcionamiento esperado y permitir que el referente de negocio (contraparte/usuario final) determine su aceptación. Las pruebas deben ser realizadas por el referente de negocio junto al Ingeniero responsable del Proyecto y las personas que se definan pertinentes. En esta etapa, el usuario final debe plantear todas las deficiencias o errores del sistema, antes de aprobar su paso a ambiente de producción.

El Ingeniero responsable del proyecto en LA OFICINA DE GESTIÓN TECNOLÓGICA E

INFORMÁTICA deberá:

- Definir los flujos de negocio que se utilizarán para validar la funcionalidad de sistema.
- Preparar ambiente y set de pruebas.
- Realizar pruebas respectivas, comparando resultados contra los esperables para cada flujo de negocio definido.
- Documentar cada prueba realizada y dejar evidencia en carpeta de proyecto.
- Coordinar revisión de un representante de la sección de análisis e inteligencia de negocios, de forma previa a que solicitud sea enviada a contraparte de negocio.
- Consensuar con contraparte de negocio los criterios de aceptación de cada prueba.

El Ingeniero asignado de la sección de análisis e inteligencia de negocios de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA deberá:

- Realizar pruebas respectivas, comparando resultados contra los esperables para cada caso flujo de negocio definido.
- Documentar y comunicar al responsable del proyecto el resultado de las pruebas realizadas.
- Aprobar la resolución de las pruebas, lo que permitirá continuar con las pruebas de contraparte de negocio.

La contraparte de negocio deberá:

- Realizar pruebas respectivas, comparando resultados contra los esperables para cada caso de uso definido
- Documentar y comunicar a responsable del proyecto el resultado de las pruebas realizadas.
- Aprobar la resolución de las pruebas, lo que permitirá al responsable de proyecto cerrar etapa y pasar el sistema a ambiente de producción.

Paso a producción

Una vez resueltos los problemas detectados en la etapa anterior, la aplicación desarrollada se pasará al ambiente de producción, donde quedará a disposición de los usuarios finales. Se deberá considerar un período de marcha blanca, para solucionar problemas no identificados en la etapa de pruebas. Luego de ello, las partes involucradas firmarán el acta de entrega final del producto.

En particular, en caso de que se trate de una actualización de un sistema existente (en producción), el responsable del proyecto deberá realizar las siguientes tareas:

- Solicitar autorización, vía correo electrónico, para paso a producción al Coordinador de proyectos con copia al Encargado Desarrollo.
- Revisar y ejecutar checklist de paso a producción definido por LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA (ver Anexo 4). Notificar a la Contraparte

de la dependencia del paso a producción. La notificación deberá ser a través de correo electrónico el cual además debe copiar a coordinador de proyecto y encargado desarrollo, indicando lo siguiente:

  - Día
  - Hora
  - Tiempo estimado de duración
  - Cambios a realizar

- Realizar un respaldo de sistema en producción previo a la ejecución de la actualización del mismo,
- El nombre del respaldo debe contar con una identificación clara indicando el nombre de sistema y fecha de respaldo. El nombre del archivo de respaldo se compone de la siguiente forma: NOMBRESISTEMA_AAAAMMDD_HHMM (Ejemplo: SistemaXYZ_20160513_1545)
- Si paso a producción requiere de alguna modificación de la base de datos, o bien, por la naturaleza de la actualización se requiere respaldar los datos del IMRDS, el responsable del proyecto deberá coordinar con el Administrador de base de datos para que este último realice un respaldo de la Base de datos.
- El nombre del respaldo debe contar con una identificación clara indicando el nombre de la base de datos y fecha de respaldo. El nombre del archivo de respaldo se compone de la siguiente forma: NOMBREBASEDEDATOS_AAAAMMDDHH_MM (Ejemplo: BaseDatosXYZ_20160513_1545)
- Revisar y modificar todos los elementos de adaptación del software para paso a producción, entendiéndose como tal todos los cambios de direccionamiento que deben realizarse para que aplicativo funcione correctamente en producción.
- Elementos a revisar:
  - String de conexión hacia servidor y base de datos de producción.
  - Dirección de carpetas relacionadas al software para recopilación de documentos.
  - WebServices utilizados por sistema deben apuntar a servidores de producción.
  - Direcciones de correo electrónico de alerta deben ser los destinatarios definidos para producción.
  - Cualquier otra variable de esta índole que al pasar de desarrollo/testing a producción debe ser chequeada.

Pasos durante el paso de producción:

- El Administrador de base de datos habilitará acceso restringido al responsable del Proyecto (previa solicitud hecha con anticipación) quién deberá crear o actualizar la base de datos con aprobación y asistencia del Administrador de Base de Datos.

- El responsable del Proyecto deberá copiar los archivos del aplicativo en la carpeta correspondiente en el Servidor de Archivo, una vez concluida correctamente el Cheklist de paso a producción.

Pasos posteriores a paso a producción:

- Realizar revisión de sistema en producción para ver la correcta ejecución de los cambios realizados en el mismo. Pruebas deben estar acorde a solicitud inicial de cambio por parte de contraparte (plan de proyecto, mejora de sistema o soporte de sistema).
- Documentar paso a producción (checklist) en carpeta de sistema (digital y papel). Notificar, a través de correo electrónico, paso a producción correctamente ejecutado a coordinador de proyectos, encargado desarrollo y usuario final.

Cambios de emergencia – Error de Sistema

El proceso de cambio de emergencia abarca todo problema o error que esté afectando la operatividad de un sistema en producción, por lo cual su corrección debe realizarse con la máxima celeridad posible, para no afectar la operación del IMRDS o bien provocar el menor impacto posible.

Notificación y asignación:

Las actividades consideradas son las siguientes:

- Unidad Administrativa debe identificar el problema e, idealmente, la corrección propuesta, en la medida que sea posible.
- Desde LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA se asignará la solicitud al jefe de Proyecto o al desarrollador específico para dar respuesta a la emergencia.
- Se deberá evaluar en conjunto con la contraparte del área solicitante, la necesidad de realizar testing, antes de pasar la solución a producción.

Pruebas

El Ingeniero responsable de proyecto deberá:

- Realizar pruebas respectivas, comparando resultados contra los esperados.
- Documentar cada prueba realizada con “Documento de Evidencia de Pruebas” y dejar evidencia en carpeta de proyecto.
- Consensuar con contraparte del negocio los criterios de aceptación de cada prueba.

Paso a producción

- Publicar solución en ambiente de producción, de acuerdo a lo especificado en sección 3.2.5.1.6.
- Documentar cambio realizado en aplicación, detallando origen de cambio, solución y fechas respectivas.

Mejoras de Sistema

Se entenderá como mejoras de sistema aquellas funcionalidades o condiciones que se solicitan con objeto de refinarlo, pero que no tienen asociados errores como los descritos en la sección 3.2.5.2, y que, además, su implementación no requiera modificaciones al modelo de bases de datos o una dedicación exclusiva mayor a una semana (ejemplos: cambiar nombres de columnas en una tabla; agregar información disponible a una vista particular que no la contiene; cambiar criterio para ordenar información según nombre o fecha; etc.). Estas solicitudes deberán ser abordadas solo en caso de que existan los recursos disponibles, de modo de no poner el riesgo el desarrollo de la planificación anual, ni los servicios de soporte relacionados con la resolución de los errores de sistema.

Notificación y asignación

Las actividades consideradas para este tipo de cambio son las siguientes:

- En caso de detectarse una mejora relevante, la dependencia correspondiente deberá realizar la respectiva solicitud.
- Desde LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA se asignará la solicitud al jefe de Proyecto o al desarrollador específico para su evaluación. Se deberá comunicar factibilidad de implementación al área solicitante, de acuerdo a la planificación de actividades establecida. En caso que la solicitud no cumpla las condiciones establecidas como mejora de sistema, el área solicitante deberá gestionarla como un desarrollo nuevo, de acuerdo a lo indicado en la sección 3.2.5.1.
- Se deberá evaluar en conjunto con la contraparte del área solicitante, la necesidad de realizar testing, antes de pasar la mejora a producción.

Pruebas

El Ingeniero responsable del proyecto deberá:

- Realizar pruebas respectivas comparando resultados contra los esperados.
- Documentar cada prueba realizada con “Documento de Evidencia de Pruebas” y dejar evidencia en carpeta de proyecto.
- Consensuar con contraparte de negocio los criterios de aceptación de cada prueba.

Contraparte de Negocio debe cumplir con:

- Realizar pruebas respectivas comparando resultados contra los esperados.
- Documentar y comunicar a responsable de proyecto resultado de pruebas realizadas.
- Dar aprobación a pruebas una vez se cumplan satisfactoriamente cada una de ellas, lo que permitirá a responsable de proyecto cerrar solicitud de mejora.

Paso a producción

- Publicar mejora en ambiente de producción, de acuerdo a lo especificado en sección 3.2.5.1.6.

Cambios mayores de sistemas

Se considerará como cambio mayor toda solicitud de modificación de un sistema, que no corresponda a los cambios indicados en las secciones 3.2.5.2 y 3.2.5.3. Estas solicitudes deberán ser gestionadas como un desarrollo nuevo, de acuerdo a lo indicado en la sección 3.2.5.1.

Estándares de desarrollo

Para el desarrollo de Sistemas de Información se deberán considerar las siguientes condiciones.

Lenguaje de Programación

- Se deberá utilizar el lenguaje de programación #C, en la plataforma .NET, con el objetivo de estandarizar los sistemas y aplicativos creados internamente y aquellos que se externalicen. Solo en casos excepcionales y bajo la aprobación del LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, se podrán utilizar lenguajes de programación alternativos.
- Se dispondrá de un entorno de desarrollo integrado, afín al lenguaje antes mencionado.

Bases de Datos

- Se utilizará como motor de base de datos las tecnologías de MySQL y ORACLE Database y SQL SERVER en su versión más actualizada, según disponibilidades técnicas y presupuestarias. Solo en casos excepcionales y bajo la aprobación del LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, se podrán utilizar motores de datos alternativos.
- Solo personal del LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA tendrá acceso a las bases de datos.
- La creación y/o modificación de las bases de datos deberá realizarse, según las normas y estándares que establezca el LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA para estos fines.

Gestión de código fuente

El código fuente corresponde a un conjunto de instrucciones, a través de líneas de texto, que determinan la ejecución de una aplicación específica, como por ejemplo un Sistema de Información. Para una gestión eficiente del código fuente, se hace necesario controlar el acceso y el uso de un mecanismo de control de versiones, el cual tiene asociado una serie de beneficios: mantener información de historial detallada sobre los cambios de elementos; administrar fallos, permitiendo la recuperación de versiones anteriores; y permitir la colaboración entre diferentes proyectos y desarrolladores, a través del uso compartido de elementos.

A continuación, se describen los dos tipos de controles que deben ser considerados:

Control de accesos:

- El control de acceso al código fuente de los programas y/o aplicaciones disponibles en el IMRDS, debe estar restringido sólo al personal de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, para evitar la intervención de terceros no autorizados.
- En los casos en que terceros requieran acceder al código fuente, se deberán verificar sus competencias para ello y deberán ser supervisados por personal de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA.

Control de versiones:

- Se deberá utilizar el sistema de control de versiones adoptado por el LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA de la Superintendencia del Medio Ambiente. Los desarrolladores deberán estar identificados y tendrán la obligación de aplicar control de versiones en todos los proyectos en que se desempeñen.
- Será responsabilidad de cada jefe de Proyecto el otorgar los accesos necesarios al código fuente de cada uno de sus proyectos iniciados por el IMRDS.
- Cada proyecto que se desarrolle deberá contar con dos repositorios, uno para almacenar el código fuente de la aplicación construida, la cual deberá pertenecer y ser mantenida a través del sistema de control de versiones, y otro para toda la documentación asociada a la creación y mantención de la aplicación, de acuerdo a los procedimientos y estándares definidos por el IMRDS, la cual deberá estar disponible y actualizada.
- Los repositorios deberán ser creados por el jefe de Proyecto asignado u otra persona que sea asignada para tales fines, cuando se confirme el comienzo del proyecto. Será responsabilidad de cada jefe de Proyecto mantener actualizados los dos repositorios indicados.

Definición de Ambientes

Se utilizarán tres ambientes para el desarrollo de aplicativos.

Ambiente de Desarrollo

- Ambiente donde se creará el aplicativo.
- Este ambiente deberá tener las características técnicas necesarias para el desarrollo del aplicativo.
- Bajo este ambiente se escribirá el código fuente del aplicativo y se desarrollarán las versiones de prueba, las cuales se habilitarán posteriormente en ambiente de testing.

Ambiente de Pruebas:

- Ambiente donde se prueba el aplicativo en desarrollo.
- Este ambiente debe ser una copia del ambiente de desarrollo y su objetivo es hacer pruebas de diferentes tipos. Ejemplos: pruebas de integración, pruebas de compatibilidad y pruebas de aceptación.

Ambiente de Producción:

- Ambiente final del aplicativo para uso de los usuarios.
- Este ambiente debe contener las características que tiene el ambiente de testing.
- Antes de liberar una nueva versión de un aplicativo en producción, el Jefe de Proyecto deberá respaldar las versiones vigentes del código fuente y de la base de datos, según las normas y estándares definidos por LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA para estos fines.

Tabla 1: Ficha de Proyecto

Información General del Proyecto			
* **Año Inicio Proyecto**		* **Fecha Creación**	
* **Nombre del Proyecto**			
* **Responsable de Proyecto**			

Versión	**Fecha**	**Autor**	**Razón del cambio**
1			Creación

Descripción del Proyecto	
* **Resumen Ejecutivo**.	
[Proveaunadescripcióngeneraldequédioorigendelproyecto,sualcance,supuestos,riesgos,costos,plazos, enfoque desolucióny organización.* *Si el proyecto surge como respuesta a una o más Solicitudes de Servicio, indique cuáles son.* *Recuerde que este texto será revisado por ejecutivos que no necesariamente entiende sobre tecnología, por lo que debe evitar detalles y jerga tecnológica.* *Si existe, puede hacer referencia a un PowerPoint con un resumen ejecutivo]	
* **Área Principal:**	
* **Jefe de Área:**	
* **Responsable del Área:**	
* **Necesidad y Objetivos del Negocio**	

***[Describa la necesidad que da origen al proyecto, y cómo el proyecto satisface esa necesidad.*

*Los objetivos definen los "factores de éxito" respecto de los cuales el Cliente Principal medirá si los productos o servicios producidos por el proyecto responden efectivamente a la necesidad.]***

*** Alcance y Objetivos del Proyecto**

Descripción del Proyecto

***[Los objetivos describen lo que se logrará y se entregará con este proyecto. Los objetivos tienen que ser específicos, medibles, abordables y realistas.*

*El logro de un objetivo debe ser evidente a través de la creación de uno o más entregables.]***

*** Entregables**

*[**El avances y logro de objetivos de un proyecto se hacen evidentes a través de la creación de uno o más entregables. Liste brevemente los entregables del proyecto]***

*** Qué no incluirá este proyecto**

***[En algunos casos la forma más clara de delimitar el alcance del proyecto, es enumerar explícitamente las actividades, productoso servicios que no están incluidos.*

*Liste brevemente aquellas actividades o entregables que le parece pertinente explicitar que no serán incluidos como parte del proyecto]***

*** Supuestos y Restricciones**

*[**Listar cualquier condición que pueda limitar las opciones del proyecto en cuanto a recursos, personal o plazo Ejemplos:*

- *Presupuesto predeterminado*
- *Una fecha de término inamovible*
- *Límite en el número de personas disponibles*
- *Necesidad de que se apruebe una ley antes de salir*
- *Necesidad de que se entregue un equipo para poder iniciar las pruebas]***

Hitos Bitácora de Proyecto.

*** Relación con Proveedores (marque con una X):**

No hay proveedores externos	**x**	**Llamado a Propuesta**	
Continuación de Contrato		**Existe un Único Proveedor**	

#	Fecha	Hito	Observación
1	*Aaaa-mm - dd*	*Especificación de Requerimientos (indicar hitos correspondientes a la etapa)*	
2	*Aaaa - mm-dd*	*Plan de Proyecto (indicar hitos correspondientes a la etapa)*	
3	*Aaaa - mm-dd*	*Construcción/Desarrollo (indicar hitos correspondientes a la etapa*	
4	*Aaaa - mm-dd*	*Pruebas (indicar hitos correspondientes a la etapa)*	
5	*Aaaa - mm-dd*	*Cierre y entrega (indicar hitos correspondientes a la etapa)*	

Estimación de Tamaño	
* **Costo total estimado en cantidad y moneda (Proyectos externos)**	
* **Plazo total estimado en cantidad semanas**	
* **Esfuerzo total estimado en HH**	

Lista de anexos y documentos adjuntos (carpeta digital y física)	
Descripción del documento	**Ubicación y nombre o hipervínculo**

Involucrados

Notas

* LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA			
Nombre	**Cargo**	**Responsabilidad**	**HH/MES**
*** Otras Áreas**			
*** Proveedores o Personal Externo**			
*** Áreas relacionadas**			
Área u organización	**Relación**		
*** Proyectos relacionados**			
Nombre Proyecto	**Relación**		

Tabla 2: Formato de set de pruebas

Sistema:	<Identificador del proyecto>

Información General	
Identificador de Flujo de Negocio:	<Identificador del flujo de negocio a probar>
Nombre de Flujo de Negocio:	<Nombre del Flujo de Negocio a probar>
Descripción Prueba:	<Descripción de la prueba que se va a realizar>
Responsable:	<Nombre de persona que ejecuta la prueba>
Ambiente de Prueba (Basededatos/Servidor/URL)	<Descripción de ambiente en donde se realizarán la prueba>
Prerrequisitos	

<Prerrequisitos que se deben cumplir para iniciar la prueba>

Descripción de Casos de Prueba				
Caso: <Explicación breve del caso de prueba a ejecutar*.>				
Instrucciones de Prueba <Pasos que se deben seguir para poder realizar correctamente la prueba>				
Escenarios de prueba			**Respuesta esperada de la aplicación**	**Coincide (Si/No)**
Campo	**Valor**	**Tipo escenario**		
<Nombre decampo aprobar>	<Dato de prueba>	<Correcto/ Incorrecto>	<Descripción completa de respuesta que debe dar la aplicaciónalusar elcampo especificado con el dato de prueba>	<sí/no, según la respuesta obtenida>
Criterios de Aceptación <Lista de chequeo de las condiciones que se deben cumplir para aprobar el caso de uso que se está probando.>				
Evidencia <Evidencia de prueba realizada y resultado de esta (ilustración).>				

Tabla 3: CheckList paso a producción

Fecha/Hora	
Responsable	

Identificación de Sistema	
Nombre	
Contraparte	
Área solicitante	

Ambiente de Paso a Producción	
Servidor	
Base de Datos	
URL Sistema	

Procedimiento					
		CUMPLE			
#	**Aspecto Verificado**	**SI**	**NO**	**N/A**	**Observaciones**
Pasos Previos a paso a producción					
1	Solicitar autorización paso a				

	producción				
2	Notificación a contraparte previa a paso a producción.				

3	Realizar respaldo de sistema previo a paso a producción.				
4	Realizar respaldo de base de datos previo a paso a producción.				
5	Verificar que se encuentren previamente todos los elementos de adaptación de sistema a producción correctos.				
6	Revisar string de conexión de código fuente que debe apuntar a base de datos de producción.				
Pasos durante paso a producción					
5	Modificación de base de datos en servidor de producción				
6	Actualización de código fuente en servidor de producción				
Pasos posteriores a paso a producción					
7	Revisión de correcta conexión de sistema y visualización de cambios efectuados.				
8	Notificar paso a producción ejecutado satisfactoriamente con la contraparte.				
9	Documentación de paso a producción respaldada en papel y digitalmente.				

N/A: No Aplica

6.7 Procedimiento de Respaldos de la Información

6.7.1 Introducción

La información es el activo principal del IMRDS para la continuidad operativa de sus procesos y servicios. Ante eventos adversos, es esencial mantener respaldada la

información y contar con mecanismos de recuperación.

El respaldo de información corresponde a la copia de datos de un dispositivo primario en uno o varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra un desperfecto electromecánico o un error en su estructura lógica, sea posible disponer de la mayor parte de la información necesaria para la continuidad operacional y evitar pérdida generalizada de datos.

6.7.2 Objetivo general

Establecer las directrices de respaldo y recuperación de información, con objeto de proteger los datos y sistemas necesarios para la continuidad operacional del IMRDS.

6.7.3 Alcance

Este procedimiento define la información que se respalda en el IMRDS y es aplicable a todos los funcionarios (planta - contratistas) y terceros que presten servicios a el IMRDS.

6.7.4 Responsabilidades

Para cumplir los objetivos del presente procedimiento, se establecen los siguientes roles y responsabilidades.

6.7.4.1 la oficina de gestión tecnológica e informática

Le corresponderán las siguientes responsabilidades:

- Disponer de un mecanismo de respaldo de información. Se deberán realizar mantenciones y actualizaciones de equipos y licencias que correspondan, con objeto de evitar problemas en el funcionamiento de este mecanismo.
- Realizar el respaldo de información, de acuerdo a lo establecido en este procedimiento, velando por el cumplimiento de los tres principios básicos de la seguridad de la información: integridad, confidencialidad y disponibilidad.
- Evaluar lineamientos, herramientas y soluciones informáticas, con objeto de hacer un uso eficiente de los recursos disponibles para el respaldo de la información.
- Asistir a los funcionarios y colaboradores del IMRDS, ante la necesidad de orientación con respecto al respaldo de información.

6.7.4.2 personal del IMRDS

Le corresponderán las siguientes responsabilidades:

- Respaldar la información contenida en sus computadores asignados. En particular, deberán respaldar la información estratégica para su dependencia. Queda estrictamente prohibido guardar archivos personales.

6.7.5 Descripción del procedimiento

6.7.5.1 Consideraciones generales

- Se deberán respaldar todos los Sistemas de Información existentes en el ambiente de producción, incluyendo sitios web, documentos electrónicos, bases de datos y códigos fuentes.

- Se deberán respaldar todos los correos electrónicos.
- Se deberán disponer carpetas en la red del IMRDS para los distintos equipos de trabajo, de modo que puedan almacenar en ellas la información relevante para desempeñar sus funciones. Estas carpetas deberán ser respaldadas.
- Se deberán respaldar los documentos contenidos en los computadores de usuarios desvinculados.
- Las claves de usuarios no serán respaldadas.
- La información que no sea relevante para el Instituto no será respaldada, de acuerdo a lo que establezca el Comité de Seguridad de la Información.
- Para realizar los respaldos se deberán utilizar las herramientas y normas que establezca el LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA.
- Cada respaldo que se realice deberá quedar registrado en los logs de los servidores.

6.7.5.2 Medios de respaldo

- El uso de los servidores de respaldo será destinado exclusivamente para apoyar las funciones propias del IMRDS, quedando estrictamente prohibido almacenar cualquier otro tipo de información.
- Si un medio de respaldo se encuentra próximo a su vencimiento, se deberá traspasar la información contenida en él a otro medio de respaldo.
- Ante cambios tecnológicos venideros, se deberán evaluar impactos sobre los medios de respaldo y tomar las medidas que correspondan con antelación, de modo de proteger la información contenida en ellos.
- Se deberán considerar respaldos adicionales para la información estratégica del IMRDS. En particular, esta información deberá ser respaldada, idealmente, en un edificio distinto al del nivel central del IMRDS, en el cual se encuentra la sala de servidores del IMRDS, con objeto de evitar pérdidas provocadas por incendios, inundaciones, terremotos, entre otros incidentes. La copia externa se podrá implementar en una o más oficinas regionales o, idealmente, en un datacenter especializado, en la medida de que existan los recursos disponibles para ello.
- La información contenida en los servidores que no sea necesaria para el IMRDS deberá ser borrada, de acuerdo a lo que resuelva.

6.7.5.3 Recuperación

Se deberán realizar pruebas de recuperación de los respaldos, a lo menos una vez por semestre. Estas pruebas consistirán en la restauración de los sistemas que correspondan, a partir de su respaldo, y deberán quedar debidamente documentadas. En caso de presentarse problemas durante las pruebas, se deberán implementar las medidas correspondientes para prevenir su ocurrencia en el futuro.

6.8 Procedimiento de Seguridad de Oficinas e Instalaciones

6.8.1 Introducción

El IMRDS cuenta con distintos espacios sensibles en términos de manejo de información electrónica y sistemas informáticos que deben ser resguardados.

6.8.2 Objetivo

Establecer directrices para el control de acceso a las instalaciones del IMRDS, con objeto de resguardar la información relevante para el desempeño de sus funciones.

6.8.3 Alcance

El presente procedimiento es de carácter obligatorio para todo el personal que tenga acceso a las instalaciones del IMRDS.

6.8.4 Responsabilidades

Para cumplir los objetivos del presente procedimiento, se establecen los siguientes roles y responsabilidades.

6.8.4.1 La oficina de gestión tecnológica e informática

Le corresponderán las siguientes responsabilidades:

- Velar por el cumplimiento de este procedimiento.
- Administrar el sistema de video vigilancia, disponible en las oficinas habilitadas para ello, el cual deberá estar operativo permanentemente y cubrir los principales accesos del IMRDS, debiendo mantener grabaciones de al menos las últimas 2 semanas. Además, deberá mantener un registro de quienes, bajo autorización de las jefaturas correspondientes, accedan a las grabaciones de las cámaras.
- Administrar accesos a los equipos de servidores y equipos de comunicaciones.
- Administrar la entrega de carnets para acceder a las dependencias del IMRDS, en las oficinas que corresponda.

6.8.4.2 Personal del IMRDS

Le corresponderán las siguientes responsabilidades:

- Cumplir lo establecido en este procedimiento, velando por la seguridad de las oficinas, espacios y medios del IMRDS, en particular, dando aviso a quienes correspondan ante situaciones sospechosas que pudiesen representar un riesgo a la seguridad de la información del instituto.

6.8.5 Descripción del procedimiento

6.8.5.1 Acceso a oficinas del IMRDS

- Toda persona externa a el IMRDS deberá ser recibida en la recepción por el personal designado para ello, debiendo identificarse y comunicar las razones de su visita. Quienes accedan a espacios interiores, solo podrán transitar por los espacios autorizados para su visita.
- Para que un funcionario y/o colaborador del IMRDS pueda ingresar a sus dependencias, deberá poseer un carnet de visitante, la cual será proporcionada por la persona que se encuentre encargada en recepción, al momento de vincularse a el IMRDS.

6.8.5.2 Acceso a servidores y equipos de comunicaciones

- Solamente personal del LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA estará autorizado para acceder a los espacios donde se encuentren servidores y equipos de comunicaciones, teniendo a cargo la administración de los controles de acceso correspondientes.
- En caso de requerir soporte de personal externo (proveedores y consultorías), siempre deberá estar presente un profesional de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, mientras se estén realizando las obras y/o actividades.

6.8.5.3 Acceso a bodega informática

- Solamente personal de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA estará autorizado para acceder a la bodega o los espacios disponibles para almacenar equipos de computación y otros elementos relacionados.
- El pasillo para acceder a las bodegas debe estar despejado para su libre tránsito.

6.9. Procedimiento de Seguridad de Redes

6.9.1. Introducción

El IMRDS maneja información que debe ser protegida para llevar a cabo correctamente sus funciones. Para ello se deben implementar controles que aseguren la integridad, confidencialidad y disponibilidad de la información dispuesta en la red institucional.

6.9.2. Objetivo

Establecer directrices para el control de acceso a las redes, así como la protección contra servicios conectados no autorizados.

6.9.3. Alcance

Este procedimiento define controles de acceso a las redes del IMRDS y es aplicable a todos los funcionarios (planta - contratistas) y terceros que presten servicios al IMRDS.

6.9.4. Responsabilidades

Para cumplir los objetivos del presente procedimiento, se establecen los siguientes roles y responsabilidades.

6.9.4.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

Le corresponderán las siguientes responsabilidades:

- Velar por el cumplimiento de este procedimiento.
- Administrar accesos a las redes del IMRDS.
- Asistir al personal del IMRDS con respecto al acceso a redes del IMRDS.
- Definir los aspectos técnicos y velar por el cumplimiento de los servicios establecidos en los contratos de Internet, telefonía y enlaces MPLS (Multiprotocol Label Switching).

6.9.4.2. Personal del IMRDS

Le corresponderán las siguientes responsabilidades:

- Cumplir lo establecido en este procedimiento, velando por la seguridad de las redes de información del IMRDS.
- Mantener reserva de las claves de acceso a las redes del IMRDS.

6.9.5. Descripción del procedimiento

6.9.5.1. Terminología

- VPN (Virtual Private Network o en español Red Privada Virtual): es una tecnología de red que permite una extensión segura de la red local LAN sobre una red pública o no controlada como internet.
- Router (enrutador): dispositivo que permite enviar o encaminar paquetes de datos en una red a otra, es decir interconectar subredes.

- Firewall (cortafuegos): dispositivo que permite bloquear el acceso no autorizado, como también permitiendo acceso a comunicaciones autorizadas.
- Switch (conmutador): dispositivo que permite interconectar dos o más segmentos de red.
- WEP (Wired Equivalent Privacy o Privacidad Equivalente al Cableado): es un sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes inalámbricas que permite cifrar la información que se transmite.
- WPA (WI-FI Protected Access o Acceso WI-FI protegido): es un sistema para proteger las redes inalámbricas WIFI, creado para corregir las deficiencias del sistema previo WEP.
- WPA2 (WI-FI Protected Access 2 o Acceso WI-FI protegido 2): es un sistema para proteger las redes inalámbricas WI-FI, creado para corregir las vulnerabilidades en WPA.
- IPsec (Internet Protocol security o Seguridad en Protocolo Internet), es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el protocolo de Internet (IP) autentificando y/o cifrando cada paquete IP en un flujo de datos.

6.9.5.2. Administración de la red y de equipos de conectividad

- Todos los usuarios que accedan a la red deberán contar con una identificación única que son las credenciales de acceso del servicio de directorio, proporcionada cuando ingresan a el IMRDS.

- Las contraseñas de red deberán cumplir con los siguientes requisitos:
  - Longitud de contraseña mínima 8 caracteres.
  - Uso de mayúsculas y minúsculas.
  - Uso de al menos un carácter especial. Ejemplos: puntos, asteriscos, guiones, etc.
- Las contraseñas de red WIFI no deberán tener encriptación WEP O WPA, sino que encriptaciones WPA2 o superior.
- Todos los dispositivos de comunicaciones (Routers, Firewall, Switches) deberán tener contraseñas únicas. solo los funcionarios de la sección de Infraestructura y redes de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA podrán tener acceso remoto a los equipos de conectividad (Router, Switch, Access point, etc.).
- No se deberá permitir la configuración de los equipos de conectividad a través de conexiones inalámbricas.
- Se deberá mantener un listado de accesos inalámbricos identificados con sus claves, ubicaciones, alcances, responsables, usuarios, etc.
- Acerca de la administración y protección del enrutamiento de la red IMRDS, se deberá evitar la transmisión de los datos incompletos, la divulgación no autorizada y la duplicación o repetición no autorizada del dato.

6.9.5.3. Acceso lógico al dominio LOCAL

- Todo funcionario y colaborador del IMRDS deberá contar con una cuenta de usuario para poder acceder a los servicios de correo electrónico y otros recursos de red. La solicitud para ello deberá ser gestionada según lo establecido en el procedimiento de asignación de equipos y acceso a los sistemas de información.
- Se deberán establecer perfiles para la creación de cuentas de usuario en el dominio de red LOCAL, según las funciones y recursos correspondientes, incluyendo casilla de correo electrónico institucional.
- El formato de las cuentas de usuario deberá ser el siguiente: <primera letra del nombre><apellido paterno>. Si existe coincidencia entre dos funcionarios que tienen nombres y apellidos iguales, se agregará la primera letra del apellido materno al final del apellido paterno, es decir <primera letra del nombre><apellido paterno><primera letra apellido materno>.
- Todo funcionario que tenga asignado un equipo personal, deberá ingresar sus credenciales en la ventana de control de acceso de su equipo. De igual manera, podrá utilizar dichas credenciales cuando quiera acceder a su correo electrónico desde Internet (servicio G-Suite) a través de la URL http://mail.google.com
- Dado que la información contenida en los equipos personales de los funcionarios también se considera sensible para el IMRDS, se ha implementado un esquema de bloqueo de la sesión de usuario, cuando este no haya generado actividad en el equipo durante un periodo de 3 minutos. Esto evita la probabilidad de robo de información y otro tipo de incidentes. Para activar la sesión, los funcionarios deberán ingresar nuevamente sus credenciales del dominio.
- Cuando un funcionario y/o colaborador haya dejado de prestar servicios a el IMRDS, la Sección de Recursos Humanos deberá informar a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, de manera de proceder a respaldar toda su información electrónica (documentos y archivos en computador personal). Por defecto, la cuenta de usuario quedará deshabilitada, lo que significa que el funcionario no podrá ocupar los recursos tecnológicos del IMRDS. Para dejar habilitada la cuenta de usuario del funcionario retirado por un período determinado, se deberá justificar e informar a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA. Los archivos digitales del funcionario retirado, tendrán una retención en los esquemas de respaldo y recuperación del IMRDS por un periodo de 4 años, al menos.
- Trimestralmente los profesionales de tecnologías deberán revisar y mantener los niveles de acceso, perfiles y privilegios de las cuentas de usuario de los funcionarios.

6.9.5.4. Acceso lógico a los sistemas de información

- Todo sistema de información que tenga una componente de gestión de procesos interna, del tipo flujos de trabajo o registros de información, deberá tener un mecanismo de control de acceso, mediante uso de credenciales de acceso (nombre de usuario y contraseña), conexión con el servicio de directorio del dominio LOCAL o

uso de certificados electrónicos.

- Si bien la administración de los perfilamientos y atribuciones en los sistemas de información es constante, anualmente se deberán revisar los niveles de acceso, perfiles y privilegios para asegurar las consistencias entre usuarios, perfiles y el ambiente operativo en aquel momento del tiempo.
- En relación con el intercambio de información e interoperabilidad con otros servicios públicos del estado y la ciudadanía, se deberá hacer cumplir la normativa vigente y las especificaciones técnicas respectivas (autenticación, encriptación, etc.), incluyéndolas en las bases de licitación cuando corresponda.

6.9.5.5. Administración del acceso remoto (VPN)

- El acceso remoto (desde internet) a la red del IMRDS deberá realizarse de forma segura y controlada, utilizando un esquema de conexión denominado VPN (red privada virtual), con protocolo de autentificación y cifrado IPsec, validando la autentificación en el servidor de directorio.
- Los accesos remotos deberán ser autorizados por el secretario de la dependencia y/o el dueño del Sistema o Aplicación que corresponda, e informados a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA. Para ello, deberán generar un ticket en la plataforma web http://172.16.0.94.
- Se podrán dar accesos temporales a personal externo a el IMRDS, solo en casos excepcionales y justificados.

6.9.5.6. Acceso lógico al punto de acceso inalámbrico (WIFI)

- El punto de acceso (conocido como Access Point) deberá ser manipulado solamente por personal de la sección de Infraestructura y Redes de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA.
- Personas externas al IMRDS tendrán acceso a la red WIFI del IMRDS, solo en casos excepcionales y justificados.
- El personal de la sección de Infraestructura y Redes de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA deberán cambiar la contraseña del identificador de red de la WIFI en periodos anuales, utilizando un esquema seguro y de fortaleza de contraseñas.

6.9.5.7. Seguridad del cableado y protección a los puertos de red.

- Todo computador conectado a través de la red cableada e inalámbrica perteneciente al IMRDS se autentificará previamente a través del protocolo IEEE 802.1X, basado en puerto, para poder acceder a internet y los diferentes sistemas en línea del IMRDS.
- Se aplicará la seguridad de puerto en las interfaces de los switches del IMRDS para evitar la conexión de más de un computador en cada puerto de red, evitando bucles

de conmutación (capa 2 del modelo OSI), lo que produciría una degradación en el rendimiento en la red cableada.

6.10. Procedimiento de gestión de Incidentes, Amenazas y Debilidades de Seguridad

6.10.1. Introducción

El IMRDS maneja información que debe ser protegida para llevar a cabo correctamente sus funciones. Para ello se debe implementar un sistema de gestión ante incidentes, amenazas y/o debilidades que puedan comprometer la seguridad de los activos de información del IMRDS.

6.10.2. Objetivo

Establecer las directrices ante la ocurrencia de incidentes o la detección de amenazas y/o debilidades que pudiesen comprometer la seguridad de los activos de información del IMRDS.

6.10.3. Alcance

El presente procedimiento aplica a todos los incidentes, amenazas y debilidades asociados a la seguridad informática y de información electrónica. No aplica a errores de funcionalidad de sistemas de información o aplicaciones de uso común del IMRDS, a menos que afecten directamente a la seguridad de dichos sistemas.

Todos los funcionarios (planta - contratistas) y terceros que presten servicios a el IMRDS deberán cumplir este procedimiento.

6.10.4. Responsabilidades

6.10.4.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

Le corresponderán las siguientes responsabilidades:

- Velar por el cumplimiento de este procedimiento, respondiendo oportunamente ante incidentes y/o amenazas, e implementando las medidas que correspondan para prevenirlos.
- Mantener registros de los incidentes y/o amenazas ocurridas, incluyendo las soluciones que se implementen.
- Realizar las mantenciones y actualizaciones que correspondan a los equipos, sistemas y circuitos eléctricos, para prevenir la ocurrencia de incidentes.

6.10.4.2. *Personal del IMRDS*

Le corresponderán las siguientes responsabilidades:

- Cumplir lo establecido en este procedimiento, velando por la seguridad de las redes de información del IMRDS.
- Informar inmediatamente a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA ante la ocurrencia de incidentes o la detección de amenazas y/o debilidades que pudiesen comprometer la seguridad de los activos de información del Instituto.

6.10.5. Descripción de Iprocedimiento

6.10.5.1. *Activos de información y tipos de incidentes*

Diversos activos de información deberán ser protegidos ante incidentes, amenazas y/o debilidades:

- Servidores.
- Equipos de conectividad (Firewall, Routers, Switches, Access points.).
- Enlaces de telecomunicaciones (Internet, MPLS, Telefonía)
- Computadores personales.
- Impresoras.
- Sistema de control de acceso y cámaras de video vigilancia.
- Central telefónica y Equipos telefónicos.
- Sistemas de información, aplicaciones y software en general.
- Cualquier otro servicio computacional entregado por el IMRDS.

Se identifican los siguientes tipos de incidentes, que pueden representar una amenaza para la seguridad de la información:

- Incendio o inundación en la sala de servidores.
- Robo de computadores personales.
- Robo de información electrónica.
- Ingreso de personal no autorizado en la sala de servidores o estaciones de trabajo de funcionarios.
- Corte eléctrico o defectos en el sistema eléctrico.
- Hacking y técnicas de suplantación.
- Virus informáticos y spyware.
- No disponibilidad de Portal institucional y sistemas de información.

6.10.5.2. *Reporte de incidentes, amenazas y debilidades de seguridad*

- Ante la ocurrencia de incidentes o la detección de amenazas y/o debilidades que

pudiesen comprometer la seguridad de los activos de información del IMRDS, se deberá da aviso inmediato a LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, incluso durante días no hábiles.

- La primera vía formal de reporte de incidentes o amenazas será mediante el envío de correo electrónico a la siguiente cuenta: soportesistemas@imrdsoacha.gov.co
- En caso de que el incidente y/o amenaza, requiera de una intervención urgente, se deberá contactar a personal de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA vía telefónica o personalmente, sin necesidad de enviar un correo electrónico.

6.10.5.3. Respuestaanteincidentes, amenazasydebilidadesdeseguridad

- Una vez recibido el incidente mediante correo electrónico, llamado telefónico o contacto personal, el profesional de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA que tome conocimiento del caso deberá informar al funcionario responsable de la infraestructura y redes de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, quien deberá iniciar una investigación.
- Detectada las causas del problema y los elementos afectados, se informará al profesional de carrera de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA sobre el plan de solución, tiempos involucrados y recursos necesarios, dependiendo del grado de complejidad y magnitud del problema, quien deberá realizar las gestiones correspondientes, incluyendo la comunicación a la SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA y las dependencias, cuando corresponda.
- Se deberá mantener un registro actualizado de incidentes y/o amenazas, incluyendo todas las acciones o medidas que se implementen para solucionarlos, ya sea de forma total o parcial.
- Mensualmente, se deberá generar un reporte de incidentes, con objeto de identificar categorías de incidentes más reportados, para luego tomar las medidas que correspondan para prevenirlos.

6.11. Procedimiento de Monitoreo de Red y Servicios

6.11.1. Introducción

Los ataques a la red interna (LAN), se pueden producir tanto a nivel externo, como a nivel interno. Por tal motivo, es necesario contar con mecanismos de monitoreo y alarmas que permitan prevenir ataques y, en caso de que ocurran, tomar acciones rápidas y oportunas, para minimizar el impacto sobre los activos de información del IMRDS.

6.11.2. Objetivo

Establecer directrices para el monitoreo de redes y servicios, con objeto de proteger los activos de información del IMRDS.

6.11.3. Alcance

El presente procedimiento considera el monitoreo de redes y servicios asociados a tecnologías de información, y es aplicable a todos los funcionarios (planta - contratistas) y terceros que presten servicios a el IMRDS.

6.11.4. Responsabilidades

6.11.4.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

Le corresponderán las siguientes responsabilidades:

- Velar por el cumplimiento de este procedimiento.
- Evaluar alternativas de mecanismos de monitoreo de red y servicios, con objeto de mejorarlos y actualizarlos, cuando corresponda.
- Realizar las pruebas, mantenciones y actualizaciones que correspondan a los equipos, sistemas y circuitos eléctricos, para prevenir la ocurrencia de incidentes.

6.11.4.2. Personal del IMRDS

Le corresponderán las siguientes responsabilidades:

- Cumplir lo establecido en este procedimiento, velando por la seguridad de las redes y servicios informáticos del IMRDS.

6.11.5. Descripción del procedimiento

- El IMRDS cuenta con los siguientes productos de hardware y software para proteger la red local y los servicios asociados.
- Firewall: Dispositivo principal que bloquea todo el tráfico entre la Internet y la red, y subredes locales.
- Antivirus: es un tipo de software cuya misión es hallar y de ser posible eliminar las amenazas detectadas a nivel de equipo final o de red.
- Para acceder a las herramientas de monitoreo de cada uno de los utilitarios y hardware, primero se deberá poseer atributos de administrador, tanto del dominio LOCAL, como de las credenciales propias que maneja cada una de las herramientas. Los únicos profesionales que poseerán dichos atributos, son los profesionales designados por LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA.
- Se deberá utilizar el primer cortafuego de la red local (Firewall), para bloquear puertos y protocolos o habilitarlos, según los requerimientos de los servicios y aplicaciones.

- Se deberá respaldar anualmente las configuraciones del cortafuego en caso de establecer un plan de recuperación ante una emergencia.
- Se deberán filtrar y observar correos de origen malicioso y de esta manera controlar los virus de correo y spyware, labor realizada automáticamente por GMAIL de Google Apps, pero supervisada por el personal de la sección Infraestructura y Redes de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, que puedan propagarse hacia los usuarios y por lo tanto, hacia la red local. Para ello, se deberán utilizar las herramientas que disponga el IMRDS.
- Se deberá monitorear todo el tráfico en la red interna, incluyendo servicios de Windows y Linux, a través de las herramientas que se disponga para ello.
- Se deberán revisar periódicamente los logs de eventos de los servicios de Windows y Linux para detectar tempranamente o, en su defecto, corregir aquellas acciones perjudiciales para la

  plataforma, los sistemas y sus activos de información.
- Los profesionales de LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA deberán realizar anualmente un análisis completo de vulnerabilidad de la plataforma tecnológica para detectar puntos débiles y generar el plan de corrección respectivo.

6.12. Procedimiento de Operaciones del Centro de Datos

6.12.1. Introducción

El Centro de Datos corresponde a un lugar debidamente acondicionado para concentrar los recursos necesarios para el procesamiento y almacenamiento de la información de una organización. Entregar niveles de servicios óptimos y de manera segura a los usuarios internos y a la ciudadanía, requiere de una correcta administración de la infraestructura y las plataformas computaciones que sustentan el Centro de Datos.

6.12.2. Objetivo

Establecer directrices para el correcto funcionamiento del centro de datos del IMRDS y para proceder ante eventos adversos que pudiesen afectarlo.

6.12.3. Alcance

El presente procedimiento considera la gestión asociada al centro de datos del IMRDS, y es aplicable a todos los funcionarios (planta - contratistas) y terceros que presten servicios a el IMRDS.

6.12.4. Responsabilidades

6.12.4.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

Le corresponderán las siguientes responsabilidades:

- Velar por el cumplimiento de este procedimiento.
- Administrar el Centro de Datos del IMRDS.
- Velar por el cumplimiento de las condiciones establecidas con los proveedores externos, con respecto al funcionamiento del Centro de Datos institucional.
- Evaluar alternativas para mejorar la configuración del centro de datos, acorde a los recursos disponibles, realizando los ajustes, actualizaciones y cambios que correspondan.
- Realizar mantenciones preventivas de los equipos.

6.12.4.2. *Personal de laIMRDS*

Le corresponderán las siguientes responsabilidades:

- Cumplir lo establecido en este procedimiento.

6.12.5. Descripción del procedimiento

Las siguientes instrucciones aplican para la sala de servidores localizada en las dependencias del IMRDS.

6.12.5.1. *Sistema Eléctrico y respaldo de energía mediante UPS*

- Sin sistema eléctrico y algún mecanismo de respaldo de energía, los enlaces y el hardware no podrían funcionar, lo cual afectaría la disponibilidad de la información. Por lo tanto, se deberá asegurar la disponibilidad de energía, dentro del alcance de los recursos disponibles.
- Se deberá contar con una fuente de alimentación monofásica independiente para suministrar energía a la sala de servidores del IMRDS. Esta fuente se deberá conectar directamente a un Sistema de Alimentación Interrumpida (conocido como UPS, por sus siglas en inglés), para entregar respaldo de energía ante un corte de la red eléctrica, con objeto de proveer el tiempo suficiente para realizar las gestiones que correspondan, para proteger los equipos que almacenan la información del IMRDS.
- Se deberá verificar que la configuración de la UPS no sea modificada, salvo que se realice una mantención. En este caso, se deberá contar con el servicio de una empresa especializada.
- Ante un corte de energía eléctrica que sobrepase las horas de disponibilidad de la UPS, los profesionales asignados por LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA, ya sea en forma presencial o remota, deberán iniciar los procesos de apagado de los equipos servidores y algunos equipos de comunicaciones, tal como se especifica en este documento, para cada uno de las componentes.

- Cuando retorne la energía, después de un corte, no se deberá realizar ningún cambio ni ajuste a la configuración de la UPS, de modo que el sistema por sí solo, comience a cargar las baterías nuevamente.

6.12.5.2. *Sistema de enfriamiento (Aire acondicionado)*

- El sistema de enfriamiento es el segundo pilar fundamental del correcto funcionamiento del centro de datos. Sin sistema de enfriamiento, existe una alta probabilidad y riesgo de que los equipos de comunicaciones y servidores fallen a causa de las altas temperaturas generadas al interior de la sala de servidores.
- Nunca se deberán cambiar las configuraciones del sistema de enfriamiento, salvo que sea justificado y estrictamente necesario.
- Cuando ocurra una falla en el sistema de enfriamiento de la sala de servidores, los profesionales del LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA deberán ingresar inmediatamente en forma presencial o remota a la consola de administración del sistema. Luego de verificar las condiciones y temperaturas respectivas, se deberán tomar medidas para bajar la temperatura de la sala y así mantener operativos los principales servicios. Si la temperatura se mantiene por sobre los 25°C, se deberá evaluar el apagado de los servidores y contactar a una empresa especialista.

6.12.5.3. *Enlace de Internet, MPLS y telefonía.*

- Sin los servicios de enlace a internet, MPLS y telefonía, el IMRDS no podría disponer del portal institucional para la ciudadanía. En tanto, para el personal del IMRDS no sería posible utilizar ciertos Sistemas de Información. Por lo tanto, se deberán tomar todos los resguardos necesarios e implementar las medidas que correspondan para permitir la continuidad operacional del IMRDS, en relación con los servicios de internet y telefonía.
- Los equipos de las empresas que proveen los servicios de internet y telefonía no deberán ser manipulados. Ante problemas asociados a su funcionamiento, se deberá dar aviso a los proveedores inmediatamente, de acuerdo a las condiciones de soporte establecidas, para que implementen las soluciones que correspondan.
- Se deberán administrar cuidadosamente los rangos de IP pública y numeraciones telefónicas que contemplen los servicios contratados.

6.12.5.4. *Equipos de comunicaciones*

- Se deberán administrar cuidadosamente las configuraciones de los equipos de comunicaciones. No se podrán realizar intervenciones a los equipos, salvo las estrictamente necesarias, como por ejemplo la habilitación de puertos y protocolos.
- Se deberá programar la ejecución de respaldos sobre las configuraciones de los equipos de comunicaciones, con objeto de preparar planes de contingencia ante

eventos adversos.

- Se deberá poner atención y especial cuidado en la administración del Firewall y la administración de las subredes creadas en dicho dispositivo. Por ningún motivo se deberá cambiar la configuración de las IP Públicas asignadas por los proveedores en el firewall.
- Se deberá monitorear la red y los servicios comprometidos, de acuerdo a lo establecido en el procedimiento correspondiente.

6.12.5.5. Equipos de servidores y cluster de virtualización

- Los servidores corresponden a las máquinas físicas, donde se almacenan las máquinas virtuales. El IMRDS cuenta con una arquitectura de Cluster de virtualización, conformado por máquinas físicas, conectadas a un SAN (Storage Area Network).
- No se podrán realizar intervenciones a los equipos, salvo las estrictamente necesarias.
- Se deberá monitorear en forma presencial o remota, las condiciones de las máquinas y los servicios entregados.
- Se deberá verificar la creación de máquinas virtuales de ambiente de producción. Para efectos de máquinas virtuales de ambiente de desarrollo o pruebas, se podrá utilizar la consola Hyper- V manager y almacenar las máquinas virtuales en los discos locales de las máquinas servidores.
- Se deberán respaldar las máquinas virtuales, tal como se especifica en el procedimiento de respaldo y recuperación.
- Se deberá verificar que los servicios montados en las máquinas virtuales se encuentren configurados correctamente en las subredes (VLAN), definidas en el Firewall. Además, se deberá verificar que los puertos y protocolos respectivos estén habilitados en el Firewall.

6.12.5.6. Equipo Storage

- Desde el punto de vista de la información y activos de documentación electrónica, el Storage es uno de las componentes principales, ya que en él residen todas las máquinas virtuales de los servicios que entrega el IMRDS (portales, servicios de seguridad por software, datos compartidos, bases de datos, sistemas de información).
- No se podrán cambiar las configuraciones del controlador del arreglo de discos, salvo que sea estrictamente necesario
- Ante cualquier falla de los discos, se deberá recurrir al soporte respectivo y seguir los procedimientos establecidos por la garantía (en caso que exista) o tener repuestos disponibles para el reemplazo de los discos duros con problemas.

6.13. Procedimiento de actualización de sistemas operativos y software

6.13.1. Introducción

Los sistemas operativos tanto de servidores de aplicaciones, como de usuarios, los sistemas de información y el software de hardware específicos, requieren constantemente ser actualizados para corregir fallas existentes o aplicar parches de seguridad.

6.13.2. Objetivo

Establecer las directrices para la actualización y aplicación de cambios de sistemas operativos y software.

6.13.3. Alcance

El presente procedimiento considera los mecanismos para actualizar y aplicar cambios sobre sistemas operativos y software, y es aplicable a todos los funcionarios, contratistas y terceros que presten servicios a el IMRDS.

6.13.4. Responsabilidades

6.13.4.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

Le corresponderán las siguientes responsabilidades:

- Velar por el cumplimiento de este procedimiento.
- Evaluar alternativas de sistemas operativos y software, con objeto de mejorarlos y actualizarlos, cuando corresponda.
- Mantener un registro de control de cambios de sistemas operativos y software.

6.13.4.2. Personal del IMRDS

Le corresponderán las siguientes responsabilidades:

- Cumplir lo establecido en este procedimiento.

6.13.5. Descripción del procedimiento

6.13.5.1. Sistemas Operativos de Servidores

- Para la plataforma de servidores Windows se deberá mantener un servicio de actualización de Windows Update denominado WSUS. Este servicio se deberá conectar con los repositorios de Microsoft en Internet para descargar las actualizaciones y parches de seguridad. Luego, se deberán distribuir los parches a los servidores y equipos de usuario, en la red local. Se deberá verificar que los equipos Windows pertenezcan al dominio LOCAL, donde está definida la política de referencia al servidor WSUS.

- Dado que algunos parches de seguridad o actualizaciones podrían afectar el correcto funcionamiento de ciertas funcionalidades tanto de Windows, como de los sistemas alojados, es recomendable revisar la documentación de la actualización o parche de seguridad, antes de aplicar a los servidores. El servidor WSUS deberá estar configurado para que las actualizaciones no se apliquen de forma automática, sino que deberán ser realizadas manualmente.
- Se deberán utilizar las herramientas de monitoreo y reportes disponibles en WSUS para conocer el estado de actualización de los equipos. Se recomienda realizar este proceso de revisión mensualmente.
- Para el caso de los sistemas operativos en ambiente Linux, la actualización y parches se realizarán en forma manual y directamente conectados a los repositorios de las distribuciones más conocidas (Ejemplo: CenTOS repo, REMI).

6.13.5.2. Sistemas Operativos de PC a funcionarios

- Al igual que los servidores Windows, los PC Windows asignados a los funcionarios, se actualizarán directamente bajando los parches de seguridad y actualizaciones desde el servidor WSUS. De esta manera, se optimiza el ancho de banda a Internet y se tiene un mayor control de las actualizaciones. Se deberá verificar que los equipos de los funcionarios pertenezcan al dominio LOCAL.
- A diferencia de los equipos servidores, las actualizaciones de los PC de funcionarios y/o colaboradores desde el WSUS se podrán programar de forma automática. Sin embargo, se les deberá dar aviso previo, para que tomen los resguardos necesarios.

6.13.5.3. Software de los servidores.

- Este tipo de actualizaciones son complejas, dado que se requieren conocimientos específicos del hardware. El funcionamiento del hardware de comunicaciones, servidores y storage requiere de configuraciones de alta complejidad, por lo que cualquier cambio puede generar efectos en cadena, con consecuencias directas sobre la operación de los sistemas y servicios que se entregan. En este sentido, se recomienda revisar las recomendaciones del fabricante y planificar proyectos de actualización, con apoyo de consultores especializados, mediante algún esquema de mantención y garantía. En todos los casos, las actualizaciones deberán estar justificadas.
- Se deberá contar con respaldo de las configuraciones, tanto de equipos servidores, como de equipos de comunicaciones, para poder afrontar contingencias.

6.14. Procedimiento de Aplicación y Control de Firmas Digitales Introducción

Para el uso de la firma electrónica, tanto en procesos internos de gestión, como para realizar acciones ante otras instituciones, es necesario establecer las condiciones generales, de

acuerdo a la normativa vigente.

6.14.1. Objetivo

Establecer las directrices generales para el correcto uso de firmas digitales en el IMRDS.

6.14.2. Alcance

El presente procedimiento considera la aplicación y control de firmas digitales, y es aplicable a todos los funcionarios (planta - contratistas) y terceros que presten servicios a el IMRDS.

6.14.3. Responsabilidades

6.14.3.1. LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

Le corresponderán las siguientes responsabilidades:

- Velar por el cumplimiento de este procedimiento.
- Evaluar alternativas tecnológicas, para la aplicación y control de firmas digitales.

6.14.3.2. Personal del IMRDS

Le corresponderán las siguientes responsabilidades:

- Cumplir lo establecido en este procedimiento.

6.14.4. Descripción del procedimiento

- Se deberá asegurar que las bases de licitación de desarrollo de sistemas de información que tramitarán procesos y documentación electrónica, señalen en forma explícita los requerimientos establecidos por la normativa de firma electrónica y seguridad del documento electrónico, cuando corresponda.
- En el proceso metodológico de desarrollo de sistemas de información se deberá determinar aquellos documentos que requerirán la aplicación de firma electrónica tanto simple, como avanzada.
- Se deberá gestionar la adquisición de certificados digitales para firma electrónica avanzada, con las entidades acreditadas tal como lo determina la ley.

- Se deberá asegurar que el proceso de firma electrónica, garantice la integridad del documento electrónico y de los repositorios donde estos se almacenarán.
- Se deberá asegurar que las comunicaciones electrónicas donde participe documentación electrónica, utilicen mecanismos de encriptación segura (certificados de sitio seguro).
- Se deberá asegurar que los sistemas de información apliquen mecanismos de No repudio para garantizar la integridad de las comunicaciones electrónicas y de los documentos propiamente tal.

7. ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

DOMINIO TI	**ROLES**
CIO (Chief Information Officer)	Jefe
Responsable de Gestión de la Información	Profesional Ingeniero de Sistemas, Especialista en Administración de Bases de Datos
Responsable de los Sistemas de Información	Profesional Ingeniero de Sistemas, Especializado en Desarrollo de Software
Responsable de los Servicios Tecnológicos	Profesional Ingeniero de Sistemas, Especialista en Gestión de Tecnología e Innovación
Responsable del seguimiento y control	Profesional Ingeniero de Sistemas, Especialista en Redes y Telecomunicaciones
Responsable de la Seguridad de la Información	Profesional Ingeniero de Sistemas, Especialista en Seguridad Informática
Responsable de la Gestión de Proyectos	Profesional Ingeniero de Sistemas, Especialista en Gestión de Proyectos

Según la guía de implementación de perfiles requeridos, definidos en el Marco de Referencia, se establecen los roles para los profesionales que cumplan con los requisitos del perfil y competencias necesarias para el desempeño de los mismos, se describen a continuación:

ROLES	DESCRIPCIÓN
CIO (Chief Information Officer)	Definir las estrategias, políticas, planes, objetivos y metas en gestión de tecnologías y sistemas de la información que faciliten el cumplimiento de la misión de cada entidad, de su sector y del Estado.
	Definir los lineamientos para el cumplimiento de estándares de seguridad, privacidad, calidad y oportunidad de la información de cada entidad y la interoperabilidad de los sistemas de información que la soportan, así como el intercambio permanente de información acorde con los lineamientos de orden nacional.
	Formular, coordinar y hacer seguimiento al plan institucional en materia de gestión de información y de la gestión de tecnologías de la información, en el marco de los lineamientos del orden nacional y territorial, cuando corresponda.
Responsable de Gestión de Información	Desarrollar estrategias para lograr un flujo eficiente de información institucional que, de un lado, promueva la rendición de cuentas ante la ciudadanía y, por otro lado, facilite tomar decisiones y cumplir los objetivos de la institución.
	Implementar el plan de la estrategia de TI en materia de gestión de información y en coordinación con el proceso de gestión de TI y en el marco de los lineamientos del orden nacional y territorial, cuando corresponda.
	Apoyar los procesos de formulación de políticas y directrices de la gestión de la información.
Responsable de los Sistemas de Información	Implementar los lineamientos y procesos de gestión de TI de cada institución en materia de software, hardware, redes y telecomunicaciones, acorde con los parámetros gubernamentales para su adquisición, operación y mantenimiento, en pro del cumplimiento de los objetivos institucionales.
	Realizar la gestión requerida para asegurar la apropiada prestación de servicios de TI, con base en los diferentes recursos asignados de software,hardware, redes, telecomunicaciones y demás.
	Implementar las estrategias, los instrumentos y las herramientas con aplicación de Tecnologías de la Información para brindar de manera constante y permanente un buen servicio al ciudadano.

Responsable de Servicios Tecnológicos	Coordinar, supervisar y asegurar la correcta operación y funcionamiento de la infraestructura y servicios tecnológicos de la institución.
	Diseñar las estrategias de apropiación de los servicios tecnológicos que ofrece la institución a los ciudadanos y los usuarios internos.
	Diseñar estrategias que incorporen las tendencias y cambios tecnológicos que sean pertinentes con los objetivos misionales de la institución.
Responsable de seguimiento y control	Velar por el cumplimiento de los lineamientos y procesos de gestión de TI de cada institución en materia de software, hardware, redes y telecomunicaciones, acorde con los parámetros gubernamentales para su adquisición, operación y mantenimiento, en pro del cumplimiento de los objetivos institucionales.
	Desarrollar y aplicar los instrumentos para medir la ejecución de las estrategias y prácticas que soporten la gestión de la información y la gestión de TI en beneficio de la prestación efectiva de sus servicios.
	Establecer herramientas de seguimiento y evaluación de los proyectos de TI implementados por la institución.
Responsable de Seguridad de la Información	Definir, seguir y controlar la estrategia informática que permita el logro de los objetivos y la minimización de los riesgos de la institución. Encargado de guiar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
Responsable de la Gestión de Proyectos	Esta función tiene por objeto la gestión de los diferentes proyectos relacionados con el diseño e implementación de esquemas de gobernabilidad de TI.
	Hacer seguimiento a los esquemas de gobernabilidad de TI de la institución, asegurando la implementación de la estrategia de TI, mediante mecanismos que permitan conectar la arquitectura misional con la arquitectura de TI.

8. INVENTARIO DE ACTIVOS DE INFORMACIÓN.

El IMRDS debe tener un profundo conocimiento sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.

- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBXs, máquinas de fax, contestadores automáticos), medios magnéticos (discos), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.
- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Estos aspectos deben tenerse en cuenta, puesto que la clasificación por exceso puede traducirse en gastos adicionales innecesarios para el IMRDS.

Las pautas de clasificación deben prever y contemplar el hecho de que la clasificación de un ítem de información determinado no necesariamente debe mantenerse invariable por siempre, y que

ésta puede cambiar de acuerdo con una Política predeterminada. Se debe considerar la cantidad de categorías a definir para la clasificación dado que los esquemas demasiado complejos pueden tornarse engorrosos y antieconómicos o resultar poco prácticos.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información.

Por último, la información puede pasar a ser obsoleta y, por lo tanto, ser necesario eliminarla. La destrucción de la información es un proceso que debe asegurar la confidencialidad de la misma hasta el momento de su eliminación.

8.1 Responsabilidad

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

8.2 Inventario de activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de no mayor a 6 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es cada responsable de Unidad Organizativa.

8.3 Rotulado de la Información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia;
- Almacenamiento;
- Transmisión por correo, fax, correo electrónico;
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

8.4 Clasificación de la información

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación, se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

8.4.1 Confidencialidad:

- Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado del IMRDS o no. PUBLICO
- Información que puede ser conocida y utilizada por todos los empleados del IMRDS y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el IMRDS, el Sector Público Nacional o terceros. RESERVADA – USO INTERNO
- Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al IMRDS, al Sector Público Nacional o a terceros. RESERVADA - CONFIDENCIAL
- Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección del IMRDS, y cuya divulgación o uso no autorizados podría

  ocasionar pérdidas graves al mismo, al Sector Público Nacional o a terceros. RESERVADA SECRETA

8.4.2 Integridad:

- Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria del IMRDS.
- Información cuya modificación no autorizada puede repararse, aunque podría ocasionar pérdidas leves para el IMRDS, el Sector Público Nacional o terceros.
- Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el IMRDS, el Sector Público Nacional o terceros.
- Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al IMRDS, al Sector Público Nacional o a terceros.

8.4.3 Disponibilidad:

- Información cuya inaccesibilidad no afecta la operatoria del IMRDS.
- Información cuya inaccesibilidad permanente durante un plazo no menor a una semana podría ocasionar pérdidas significativas para el IMRDS, el Sector Público Nacional o terceros.
- Información cuya inaccesibilidad permanente durante un plazo no menor a un día podría ocasionar pérdidas significativas al IMRDS, al Sector Público Nacional o a terceros.
- Información cuya inaccesibilidad permanente durante un plazo no menor a una hora podría ocasionar pérdidas significativas al IMRDS, al Sector Público Nacional o a terceros.
    - Al referirse a pérdidas, se contemplan aquellas mesurables (materiales) y no mesurables (imagen, valor estratégico de la información, obligaciones

contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

- CRITICIDAD BAJA: ninguno de los valores asignados supera el 1.
- CRITICIDAD MEDIA: alguno de los valores asignados es 2
- CRITICIDAD ALTA: alguno de los valores asignados es 3

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) y los perfiles funcionales que deberán tener acceso a la misma.

En adelante se mencionará como “información clasificada” (o “datos clasificados”) a aquella que se

encuadre en los niveles 1, 2 o 3 de Confidencialidad.

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA DE APROBACIÓN DD/MM/AA**	**DESCRIPCIÓN DEL CAMBIO**	**RESPONSABLE**
01	12/12/2024	Creación Plan de Seguridad y Privacidad de la Información	Líder Oficina TIC

TABLA DE APROBACIÓN		
ELABORÓ	**REVISIÓN**	**APROBÓ**
Nombre: Andres Rivas M **Cargo:** Líder de Sistemas **Firma:** *Original Firmado* **Fecha:** 12 Diciembre de 2024	**Nombre:** Cristhian Cano **Cargo:** Líder MIPG **Firma:** *Original Firmado* **Fecha:** 12 Diciembre de 2024	**Nombre:** Comité de Gestión y Desempeño Institucional **Acta N°:** 01 **Fecha:** 12/12/2024