1 OBJETIVO

Definir Lineamientos que permitan al IDEAM, asegurar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información.

2. ALCANCE

El presente manual se establecen las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas y aplicadas a nivel nacional en el marco de la operación por procesos del IDEAM y por los servidores públicos, contratistas, proveedores de servicios o a el personal que tenga alguna relación con el IDEAM.

3. NORMATIVIDAD

Ver Normograma.

4. DEFINICIONES

- **NTC-ISO/IEC 27001:2013:** Norma técnica colombiana cuyo propósito es brindar un modelo para el establecimiento, implementación, operación, seguimiento,
- revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).
- **Eficacia:** Grado en el que se ejecutan las actividades planeadas y se alcanzan los resultados esperados de la planeación.
- **Eficiencia:** Relación entre el resultado alcanzado y los recursos utilizados.

- **Efectividad:** Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.
- **Mejora continua:** Acción con el fin de aumentar la capacidad para cumplir los requisitos y optimizar el desempeño.
- **Proceso:** Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.
- **Producto o servicio:** Resultado de un proceso o un conjunto de procesos.
- **Trazabilidad:** Capacidad para seguir un historial, la aplicación o la localización de todo aquello que está bajo consideración.
- **Aceptación del riesgo**: decisión de asumir un riesgo o aceptar efectos y consecuencias.
- **Activo:** hace referencia a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, infraestructura de TI) el cual representa un valor para la entidad.
- **Activo crítico**: Instalaciones, sistemas y equipos los cuales, que, si son comprometidos, destruidos, o es degradado su funcionamiento o no se encuentran disponibles, afectaran el cumplimiento de los objetivos de una organización.
- **Acuerdos de niveles de servicio:** herramientas que permiten que los proveedores y clientes de servicios establecer un consenso en términos del nivel de calidad en la prestación y operación de un servicio, determinando, responsabilidades, garantías, tiempos de respuesta, horarios de disponibilidad, entre otros.
- **Administración de riesgos**: Proceso sistemático de identificación, control, mitigación a un costo y nivel aceptable.
- **Amenaza:** Factor potencial que tiene capacidad de generar daños, la amenaza es una condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se ocasione una violación de la seguridad.
- **Autenticidad:** Atributo de la seguridad de la información el cual busca asegurar la validez de la información en tiempo, forma y distribución.
- **Autenticación:** Procedimiento de comprobación de la identidad de un usuario al tratar de acceder un recurso informático o sistema de información.

- **Autenticación Fuerte:** Se habla de autenticación fuerte cuando un sistema de autenticación de usuario emplea a por lo menos dos de los tres mecanismos básicos de autenticación: bien sea generación de códigos PIN, credenciales, tarjetas magnéticas, token, controles biométricos.
- **Cadena de Custodia:** Aplicación de normas y/o procedimientos tendientes a asegurar, depositar y proteger cada activo de información para evitar la pérdida de integridad, disponibilidad o confidencialidad.
- **Centro de cableado**: Locación Física donde se ubican los recursos de Tecnología de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).
- **Ciberactivo**: los activos digitales como datos, dispositivos y sistemas que permiten a la organización cumplir con sus objetivos de negocio, en el ciberespacio.
- **Ciberactivo crítico**: Ciberactivo que es crítico para la operación de un servicio critico esencial para la organización.
- **Ciberseguridad**: Es la disciplina cuyo propósito es proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
- **Confidencialidad:** atributo de información que determina que la información no esté disponible ni sea revelada o divulgada a individuos, entidades o procesos no autorizados, la información es accesible únicamente a los autorizados.
- **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.
- **Control:** Medida que mantiene o modifica el riesgo.
- **CCOCI**: Comando Conjunto Cibernético, Unidad Militar Conjunta (Ejército, Armada y Fuerza Aérea), que tiene como función principal propender por la protección y el aseguramiento de la infraestructura Critica Cibernética del estado colombiano.
- **COLCERT**: Por las siglas en inglés de Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional.
- **CSIRT**: Por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-

PONAL, creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática.

- **Derechos de Autor:** conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores.
- **Disponibilidad**: Principio de la seguridad de la información que determina que los usuarios autorizados tienen acceso a la información cuando se requiera.
- **Evaluación del riesgo:** Proceso en el cual se consideran las amenazas y vulnerabilidades relativas a la información, instalaciones y probabilidad de un suceso que comprometa la confidencialidad, integridad y disponibilidad de la información.
- **Gestión del riesgo:** actividades coordinadas para dirigir y controlar una organización en lo referente al riesgo.
- **Incidente de seguridad de la información:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que pueden comprometer los principios de la seguridad de la información (Integridad, Confidencialidad y Disponibilidad).
- **Información:** Toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- **Infraestructura Crítica Cibernética (ICC)**: Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. Fuente: Ministerio de Defensa.
- **Integridad:** propiedad de salvaguardar la exactitud de la información y sus métodos de proceso y el estado completo de los activos.
- **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad
- **Líder de Seguridad de la Información:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los funcionarios del Ministerio que así lo requieran.

- **Medio removible**: Los dispositivos de almacenamiento removibles son dispositivos de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, Discos duros extraíbles, DVD y CD.
- **Mesa de Servicio**: Constituye al único punto de contacto con los usuarios finales con el fin de registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio.
- .
- **Plan de contingencia:** es un documento en el cual describe riesgos, actores, responsabilidades y los procedimientos a seguir tendientes a restablecer la operación normal, en casos de eventos adversos.
- **Plan de Continuidad de Negocio**: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones esenciales ante un evento que comprometa la operación y prestación de los servicios institucionales.
- **Plan de recuperación ante desastres: E**s un conjunto de procedimientos y acciones de recuperación de los servicios críticos misionales del IDEAM para que se pueda restablecer las operaciones en caso de un posible evento de interrupción bien sea generado por desastres natural o causado por humanos.
- **Propiedad intelectual:** es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos.
- **Propietarios de la Información:** Dependencias responsables de la generación o recopilación, custodia y preservación de la información.
- **Reasignación de derechos de acceso:** Modificación de los privilegios con que cuenta un usuario sobre un recurso tecnológico o de información.
- **Remoción de derechos de acceso:** es el bloqueo o la eliminación de los privilegios otorgados a un servicio o recursos de información a un usuario.
- **Riesgo:** Incertidumbre de un suceso que pueda generar daño o perjuicios en los objetivos de una organización.
- **Riesgo residual:** nivel de riesgo obtenido del producto de un tratamiento del riesgo.

- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.
- **SGSI:** Sistema de Gestión de Seguridad de la Información el cual busca asegurar la confidencialidad, integridad y disponibilidad de la información, basados en el ciclo PHVA.
- **Sistema de Información**: Conjunto independiente de recursos de Tecnología e información estructurado e interrelacionados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos.
- **Software malicioso:** es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse en un equipo de cómputo o una red de comunicaciones para ocasionar daños recursos informáticos, sistemas operativos, redes de datos o sistemas de información, entre otros.
- **Valoración del riesgo:** proceso global de análisis y evaluación del riesgo.
- **Vulnerabilidad:** Debilidad de un activo, Control o grupo de activos que puede ser aprovechada por una o más amenazas.
- **VPN:** Una red privada virtual de las siglas en inglés de Virtual Private Network.

5. DESARROLLO: CONTENIDO DEL MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

5.1. INTRODUCCIÓN

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, en ejercicio de sus funciones, Define el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL. El MSPI es una estrategia con el propósito de asegurar los principios de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad, otros criterios como la autenticidad y no repudio,

además de la aplicación de buenas prácticas en el marco de la operación y prestación de servicios de TI y los procesos de una organización

El presente manual hace parte integral de la resolución No Resolución 3158 de 2018, por la cual "Se Adopta la Política de Seguridad y Privacidad de la Información del IDEAM", así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la seguridad, orientados a la mejora continua y al alto desempeño a la gestión de Seguridad y privacidad de la Información.

Las políticas generales y específicas de seguridad y privacidad de la información se fundamentan en los dominios y objetivos de control de la norma ISO/IEC 27001:2013 y en el código de buenas prácticas para la gestión de la seguridad de la información ISO/IEC 27002:2015, así mismo la integración con el estándar ISO 22301:2019 como parte de las estrategias de continuidad de la operación tecnológica del IDEAM.

5.2. GENERALIDADES SGSI

5.2.1. PARTES INTERESADAS.

Las partes interesadas del Sistema de Gestión de Seguridad de la Información del IDEAM, corresponden a personas naturales o jurídicas con la cuales la Entidad interactúa en el ejercicio de sus funciones y en cumplimiento a los objetivos estratégicos y misionalidad, que pueden afectar o ser afectadas por la seguridad de la información del Ministerio y en algunos casos, pueden manifestar un interés directo, explícito y comprometido con los objetivos y propósitos del sistema de gestión de seguridad de la información - SGSI.

Parte interesada	Necesidades	Expectativas	Requisitos en el sistema de gestión	Logros y resultados esperados
Colaboradores	Socializar, apropiar y dar cumplimiento a las políticas, procedimientos y documentación del SGSI.	Cumplimiento de las políticas de Seguridad de la Información reduciendo las probabilidades de afectación a la información de la Entidad	Manual Políticas de Seguridad de la Información	Reducción de probabilidad de afectación a la información de los colaboradores
Proveedores	Socializar políticas, procedimientos y documentación del SGSI.	Cumplimiento de las políticas de Seguridad de la Información reduciendo las probabilidades de afectación a la información.	Manual Políticas de Seguridad de la Información.	Reducción de probabilidad de afectación a la información que custodie.
Usuarios				
Sociedad / Comunidad	Propender por el adecuado tratamiento de los datos personales suministrados por los usuarios que acceden a los servicios del IDEAM, de acuerdo con lo establecido en la Ley 1581 de 2012 y los	Cumplir las políticas de Seguridad y privacidad de la Información, con el propósito de preservar la información.	Manual Políticas de Seguridad de la Información	Reducción de probabilidad de afectación a la información de la sociedad y de la comunidad.
GOBIERNO				

MINTIC - Ministerio de las Tecnologías de la información y Comunicaciones	Información acerca de la ejecución de los planes, servicios, ejes temáticos, marco estratégico de TI y Gobierno Digital, así como la socialización de políticas de gobierno frente al tema de tecnología.	Colaboración y recursos para la implementación de las políticas establecidas por el ente, en relación con el componente de Seguridad y privacidad de la información de acuerdo con la estrategia de Gobierno Digital.	Lineamientos Normativa.	Cumplimiento normativo de Gobierno Digital.
Policía Nacional – DIJIN	Informe de incidentes presentados en el Instituto para su gestión siempre que sea necesario.	Suministro de evidencia digitales a la DIJIN, para el análisis forense por parte de este Ente	Manual Políticas de Seguridad de la Información.	Respuesta oportuna a incidentes de Seguridad de la Información que contemplan análisis forense.
Contraloría	Información acerca de los procesos que soliciten para su gestión.	Cumplimientos normativos.	Cumplimiento requisitos fiscales.	Evitar sanciones o hallazgos por entes de control.
Procuraduría	Información acerca de los procesos que soliciten para su gestión.	Cumplimientos normativos.	Cumplimiento de requisitos sancionatorios	Evitar sanciones o hallazgos por entes de control.
Fiscalía	Proceso de Cadena de custodia cuando se requiera	Solicitud de cadena de custodia cuando lo requiera un incidente de seguridad de la información.	Manual Políticas de Seguridad de la Información.	Respuesta oportuna a incidentes de Seguridad de la Información.
ALIADOS ESTRATÉGICOS				
CSIRT - PONAL - Equipo de Respuesta a Incidentes de Seguridad Informática	Informes de alerta de ataques que se están presentando a nivel mundial y local, y que puedan afectar a alguna entidad estatal colombiana.	Comunicación y colaboración permanente sobre el manejo de incidentes que afecten la seguridad de la información.	Manual Políticas de Seguridad de la Información.	Respuesta oportuna a incidentes de Seguridad de la Información
CCP - Centro Cibernético Policial	Ciberseguridad Ciudadana.	Investigación y Judicialización.	Manual Políticas de Seguridad de la Información	Respuesta oportuna a incidentes de

				Seguridad de la Información.
COLCERT	Ciberseguridad de Infraestructuras Críticas del país.	Coordinación de emergencias ante incidentes.	Manual Políticas de Seguridad de la Información	Respuesta oportuna a incidentes de Seguridad de la Información
CCOCI - Comando Conjunto de Operaciones Cibernéticas	Ciberdefensa de Infraestructuras Críticas Cibernética Nacional de Colombia.	Participación del IDEAM de las convocatorias de este ente para la implementación de controles a las infraestructuras críticas.	Manual Políticas de Seguridad de la Información	Ser parte del Plan Nacional de Protección de Infraestructura Crítica Cibernética del país.
SIC - Superintendencia de Industria y comercio	Registro de Base de datos en el marco de la Ley 1581 de 2012.	Cumplimientos normativos.	Cumplimento de requisito legal.	Evitar sanciones o hallazgos por entes de control.

5.2.2 COMPROMISO DE LA ALTA DIRECCIÓN

Se encargará de liderar y asegurar la implementación, sostenibilidad y mejoramiento continuo del Sistema de Gestión de Seguridad de la información - SGSI de conformidad con el alcance establecido, preservando la integridad, confidencialidad, disponibilidad de la información y continuidad de la operación de los servicios críticos institucionales de IDEAM.

5.2.3 POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

Instituto de Hidrología, Meteorología y Estudios Ambientales, adopta e implementa un Sistema de Gestión de Seguridad de la información teniendo en cuenta las buenas prácticas de estándares internacionales ISO 27001:2013 y así mismo teniendo en cuenta los Lineamientos del Modelo de Seguridad y Privacidad de la Información regido por MinTic, los cuales buscan proteger y asegurar los principios de confidencialidad, integridad, disponibilidad, autenticidad de la información y continuidad de los servicios críticos institucionales.

Es por esta razón que la Alta dirección debe aprobar y adoptar las políticas de Seguridad de la Información, contribuyendo al compromiso y aplicación de forma Integral en el marco de la operación por procesos de la entidad, igualmente El Oficial de Seguridad de la Información con el apoyo del Grupo de Arquitectura Empresarial y Seguridad de la Información - GAESI o, serán los encargados del desarrollo y mantenimiento de las políticas de seguridad, para administrar, proteger los recursos de TI y para coordinar el desarrollo de los procedimientos necesarios para ejecutar y dar cumplimiento a las políticas aprobadas. Se deberá revisar de forma periódica y de ser necesario actualizar y mejorar la política de seguridad teniendo en cuenta los diferentes aspectos organizacionales y/o legales.

El Oficial de Seguridad de la Información o quien haga sus veces con el apoyo del Grupo de Arquitectura Empresarial y Seguridad de la Información – GAESI o quien haga sus veces, serán los encargados del desarrollo y mantenimiento de las políticas de seguridad, para administrar y proteger los recursos y para coordinar el desarrollo de los procedimientos necesarios para ejecutar las políticas aprobadas.

El Oficial de Seguridad de la Información, el Grupo de Arquitectura Empresarial y Seguridad de la Información - GAES y el jefe de la Oficina de informática, de ser necesario en los comités de seguimiento proveerán un reporte escrito el cual incluirá la evaluación de las políticas, procedimientos y medidas de seguridad que están siendo adoptadas; de darse el caso un resumen de violaciones sospechosas de seguridad y las medidas adoptadas para mitigarlas.

5.3. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

5.3.1. Organización Interna

Propósito: Definir Lineamientos para gestionar a nivel organizacional la seguridad y privacidad de la información y continuidad de los servicios críticos, así como la definición y asignación de roles y responsabilidades acorde a las diferentes partes interesadas de la entidad y del sector ambiental.

Lineamientos:

- Establecer los principios, criterios y requerimientos de Seguridad de la Información que permitan asegurar la confidencialidad, integridad y disponibilidad de la información que se genera, procesa, intercambia, custodia y conserva

- La información deberá estar custodiada y preservada de acuerdo con su nivel de criticidad. Esta será responsabilidad del propietario del activo de información bien sea, director, subdirector, jefe de Oficina o coordinador de grupo o área, además de la definición y aplicación de controles para la prevención de incidentes (daño, pérdida, fuga, entre otros).

- El líder del Sistema de Gestión de Seguridad de la información de IDEAM o el Oficial de Seguridad o a quien se delegue, deberá mantener el contacto y/o alianzas estratégicas con autoridades y/o grupos de interés especial a nivel nacional e internacional referente a Seguridad de la información, de esta manera trabajar de forma conjunta para la implementación, sostenimiento y mejora del SGSI de la entidad, además de la respuesta oportuna ante incidentes que puedan generar afectación a la Entidad.

- En el marco del cumplimiento de los objetivos institucionales y en el Modelo de Operación por Procesos en la entidad, se deberá incluir y aplicar los diferentes aspectos de Seguridad de la información para la gestión de proyectos los cuales serán asesorados por el líder del Sistema de Gestión de Seguridad de la Información y Oficial de Seguridad de la Información.

5.3.2. Dispositivos Móviles y teletrabajo

Propósito: Establecer mecanismos y lineamientos para la gestión de dispositivos móviles de la entidad, el acceso a la información y condiciones de seguridad para el teletrabajo.

Lineamientos:

La Oficina de informática, deberá establecer de manera formal un proceso para el control y uso de dispositivos móviles (computadores portátiles, Tablet,

smartphone, cámaras de video digitales, entre otros), que permita orientar a los funcionarios de la entidad y terceros que requieran acceder a los servicios de TI.

- Se deberá tener un registro y control formal de los dispositivos móviles de la entidad así mismo el control para el ingreso y salida de elementos de tecnología de las instalaciones de la entidad (bitácoras o registro en sistemas de información).

- Para la salida de los dispositivos móviles propiedad de IDEAM, deberán tener una autorización previa y deberán ser protegidos mediante el uso de controles de cifrado de información y restricción de uso de aplicaciones.

- Los smartphones, propiedad de la entidad deberán disponer de sistemas de autenticación de usuarios (Patrón de desbloqueo, código de seguridad, clave o registro biométrico).

- El colaborador o responsable de la custodia del dispositivo móvil se hará responsable de este dentro y fuera de las instalaciones, igualmente de la información almacenada por tal razón deberá desarrollar mecanismos para el respaldo de información periódicamente, de ser necesario solicitar apoyo a la oficina de informática.

- Si los colaboradores hacen uso de dispositivos móviles para el ingreso a los servicios prestados por la entidad se debe prohibir el uso de dispositivos a los que se ha realizado jailbreak o similares

- Es pertinente asegurar que en caso de extravío de dispositivos se deben configurar medidas de seguridad para proteger la información corporativa (cifrado, bloqueo de pantalla, borrado remoto de datos y seguimiento de las aplicaciones ejecutadas).

- Los computadores portátiles de la entidad deberán estar incluidos dentro del dominio institucional **ideam.gov.co** para acceder a los servicios de TI, en caso de los que no son pertenecientes a la entidad, no deben incluirse en el dominio, pero se deberá solicitar la autorización mediante la mesa de servicios y cumplir con las especificaciones de seguridad dispuestas por la oficina de informática.

- Para los dispositivos móviles la oficina de Informática deberá disponer de herramientas de ofimática, antivirus, medios de almacenamiento virtual (almacenamiento en nube), herramientas de cifrado y las que se requieran siempre y cuando estas hagan parte de la línea base de software la entidad, igualmente la restricción de acceso a servicios de TI que sean considerados maliciosos y/o no hagan parte de la misionalidad de IDEAM.

- Los criterios y condiciones para ejercer la modalidad de teletrabajo deberán ser definidos de forma integral entre la oficina de Informática y el Grupo Administrativo de Desarrollo y Talento Humano GADTH, teniendo como base la normativa legal vigente mediante la formalización y/o actualización de procedimientos que incluyan los aspectos de seguridad de la información.

- Las conexiones de la modalidad de teletrabajo, remotas o por VPN, deberán ser monitoreadas y supervisadas según el perfil de usuario y/o asignación roles y privilegios, igualmente verificar la desactivación de los accesos una vez el funcionario o contratista no tenga vinculación con la entidad.

- Para los usuarios no está permitido realizar cambios en la configuración de los dispositivos móviles de propiedad del IDEAM, así mismo la instalación, desinstalación, restauración de fábrica, únicamente podrán ejecutar las actualizaciones disponibles e indicadas por la oficina de informática.

5.4. SEGURIDAD DE LOS RECURSOS HUMANOS

Propósito: Definir lineamientos que permitan a la entidad asegurar que sus funcionarios, contratistas, tengan la idoneidad y capacidad de ejercer sus funciones de acuerdo con el rol asignado, igualmente la apropiación y aplicación de las políticas de seguridad de la información.

Lineamientos:

- Los funcionarios, contratistas, aspirantes/candidatos, proveedores y ciudadanos deberán autorizar al IDEAM, el tratamiento de datos personales, de acuerdo con la normativa legal vigente, de conformidad con el Reglamento

(UE) 2016/679 ("GDPR") y la Ley 1581 de 2012, para el cual se regula el manejo de la información personal almacenada en las bases de datos, para tal fin la entidad deberá informar al titular sobre la autorización de tratamiento de datos personales.

- La entidad deberá incluir dentro de los programas de inducción y/o reinducción, sesiones de capacitación y sensibilización del sistema de gestión de Seguridad de la Información para los funcionarios y contratistas.

- Realizar la verificación del personal durante los procesos de vinculación, contratación y/o aspiración de alguna función dentro de la entidad, mediante la definición de mecanismos que permitan verificar aspectos legales, judiciales, fiscales, laborales y disciplinarios de acuerdo con la normativa legal vigente y ética pertinente, dicha documentación deberá anexarse en las historias laborales o expedientes contractuales según sea el caso.

5.4.1. TÉRMINOS Y CONDICIONES DEL EMPLEO

Propósito: Establecer lineamientos que permitan a los funcionarios, contratistas y/o proveedores dar cumplimiento a los objetivos institucionales en el marco de la gestión de la seguridad de la información.

Lineamientos:

- Definir términos y condiciones del empleo, funciones y responsabilidades frente a la seguridad de la información.

- En los procesos contractuales se deberá incluir cláusulas que permitan dar cumplimiento y contribución a la protección de los Derechos de autor, propiedad intelectual, tratamiento y protección de datos personales, acceso a la información.

- Los funcionarios, Contratistas y/o proveedores, deberán firmar como parte de sus términos y condiciones un acuerdo de confidencialidad y no divulgación de la información institucional, además de la aceptación de las políticas de seguridad de la información de IDEAM, dicho documento deberá custodiarse y preservarse en la historia laboral o expedientes contractuales según como la entidad lo establezca. Todos los colaboradores o funcionarios

deben tener actualizado el formato de compromiso de reserva y confidencialidad utilizado por la entidad

- Todos los funcionarios y contratistas deberán recibir una inducción sobre el sistema de Gestión de Seguridad de la Información, además la entidad deberá mantener registros de seguimiento.

5.4.2. DURANTE LA EJECUCIÓN DEL EMPLEO.

Propósito: Propender por la apropiación y el cumplimiento de las políticas de seguridad de la información por parte de los funcionarios y contratistas.

Lineamientos:

- Informar a todos los funcionarios y contratistas acerca de sus roles y responsabilidades en materia de seguridad de la información previo a la entrega formal de sus funciones y acceso a los recursos institucionales.

- Hacer seguimiento al cumplimiento de las obligaciones generales y contractuales, a través de los procesos de supervisión de contratos.
- Dar a conocer a los funcionarios y contratistas la documentación referente al sistema de gestión de seguridad de la información.

- Otorgar una cuenta de usuario institucional y el acceso a los servicios para la ejecución de sus funciones una vez formalizada y legalizada el proceso de vinculación laboral con la entidad, igualmente la apertura en el inventario de los bienes asignados.

- El oficial de seguridad de la información deberá diseñar y ejecutar un Plan de sensibilización, entrenamiento y comunicación, contemplando lo especificado en el Dominio de Uso y Apropiación de la Política de Gobierno Digital, el cual deberá ser dirigido a los funcionarios, contratistas y proveedores según el caso que se determine.

- La Entidad deberá disponer de un canal o medio de comunicación para realizar el reporte anónimo, que consiste en informar, denunciar y/o dar a conocer posibles incumplimientos a las políticas de seguridad de la información (denuncias internas).

5.4.3. PROCESO DISCIPLINARIO

Propósito: establecer acciones frente al incumplimiento de las políticas de seguridad de la información.

Lineamientos:

- El Instituto debe establecer un proceso disciplinario formal con el objeto de tratar los temas de los funcionarios, contratistas y/ terceras partes que se sospeche, o se ha confirmado que han cometido faltas contra la seguridad de la información, de acuerdo con las políticas y estándares definidos. El proceso debe tener en cuenta factores tales como naturaleza y gravedad de la falta, su impacto para la entidad.

- Las acciones disciplinarias no podrán establecerse, sin antes investigar y/o verificar que ha ocurrido un incumplimiento o violación a la seguridad de la información institucional.

- Todos los incidentes de seguridad de la información, deberán tener tratamiento adecuado según los procedimientos establecidos, esto con el fin de determinar causas responsables y afectaciones a la Entidad.

- En lo referente a un incumplimiento de las políticas de seguridad, y la severidad del incidente, se tomarán las acciones respectivas ante las instancias correspondientes.

5.4.4. TERMINACIÓN Y CAMBIO DE EMPLEO

Propósito: Establecer responsabilidades para la protección de los intereses institucionales, por parte de los funcionarios, contratistas y/o proveedores,

durante en proceso de terminación o cambio de empleo en materia de seguridad de la información.

Lineamientos:

- El funcionario, contratista y/o proveedor deberá entregar todos los activos de información según como lo determina el procedimiento de terminación del empleo, así mismo el proceso de entrega del cargo o separación temporal del mismo, y los informes de supervisión de contrato según el caso que aplique.

- El supervisor de contratos de cada una de las dependencias será el responsable de custodiar y preservar la información institucional, producida o generada y entregada en el marco de la ejecución de acuerdos contractuales, esto también deberá aplicarse en caso de finalización de contratos, terminaciones anticipadas, cesiones, entre otros aspectos.

- Una vez finalizada y formalizada la desvinculación laboral de algún funcionario, contratista y/o proveedor, se deberá gestionar la inactivación de la cuenta institucional y los accesos otorgados de los servicios o sistemas de información asignados, esta responsabilidad deberá ser apoyada de forma automática por el directorio activo teniendo en cuenta las fechas de ejecución contractual y vinculación laboral y soportada en un procedimiento oficial.

- Las oficinas de control interno disciplinario, gestión del talento humano, gestión jurídica en apoyo de los supervisores de contrato o quien delegue, deberán informar a la oficina de informática de manera formal (caso en plataforma de atención / mesa de servicio), las novedades en cuanto a vinculación o desvinculación laboral, contractual de algún funcionario: bien sea los diferentes motivos(desvinculación, contratación, vacaciones, licencias, terminaciones de contrato, terminación anticipadas, entre otros), una vez realizada la notificación de las novedades a la oficina de informática , procederá a la inactivación respectiva de los accesos del funcionario y/o colaborador.

- Se deberá realizar la entrega de los bienes asignados y registrados en el inventario, así mismo la devolución de cualquier distintivo institucional (prendas de vestir, morrales, carné).

5.5. GESTIÓN DE ACTIVOS

Propósito: Identificar los activos de información institucionales y definir responsabilidades de protección adecuadas.

Lineamientos:

- La entidad deberá diseñar y aprobar una metodología para la gestión de activos de información que permita identificar, clasificar y valorar los activos de información institucionales, además de la implementación de controles para preservar la confidencialidad, integridad y disponibilidad de los mismos.

5.5.1. INVENTARIO Y PROPIEDAD DE LOS ACTIVOS DE INFORMACIÓN.

Propósito: Definir lineamientos para la identificación de los activos de información de la entidad así mismo elaborar y mantener un inventario de estos.

Lineamientos:

- Se hace necesario ejercer un control sobre los elementos que generan, procesan y almacenan información en el Instituto de hidrología, Meteorología y Estudios Ambientales IDEAM, mediante el registro de la información básica de elementos físicos y lógicos que faciliten su asignación, redistribución y mantenimiento, además de establecer las necesidades en herramientas tecnológicas que se tienen en las diferentes áreas del Instituto. Mediante el inventario base del almacén o por medio de la herramienta de mesa de servicio, se mantendrá un inventario de los recursos dentro del instituto.

- Cada Proceso de la entidad deberá identificar sus activos de información pertinentes en el marco del ciclo de la vida de la información e incluir su valoración.

- Cada activo identificado, deberá ser registrado en el inventario, igualmente tener un propietario, para esta función será el líder del proceso, coordinador

de grupo, jefe de oficina, subdirector, el cual será el responsable y el encargado de coordinar y gestionar la protección de los mismos.

- La información registrada en el inventario de activos de información deberá ser íntegra y consistente, mantenerse actualizada, revisada y aprobada por los propietarios de los activos de información o con ocasión de dar cumplimiento con oportunidad a la solicitud de actualizar los activos de información para cada vigencia o periodicidad establecida por los entes de control interno del IDEAM, en cumplimiento de la ley de transparencia 1712 de 2014.

- La entidad deberá identificar los activos de seguridad digital críticos para la operación misional del instituto, de acuerdo con los criterios de valoración; determinar si deberán ser incluidos en el inventario de Infraestructura Crítica Cibernética del Sector Ambiental, estos activos deberán relacionarse con los ejercicios y estrategias de recuperación de desastres dispuestas por la IDEAM.
- El propietario de los activos de información deberá asegurarse que se encuentran registrados en el inventario, que estos se encuentren debidamente clasificados, protegidos adecuadamente y asegurarse del manejo apropiado del activo de acuerdo al ciclo de vida de la información.

    - Se define como propietario de los activos de información, líder de proceso, Subdirectores, Jefes de Oficina, Coordinadores de área, Coordinadores de grupos de las dependencias del IDEAM.

5.5.2. USO ACEPTABLE DE LOS ACTIVOS

Propósito: Definir e implementar lineamientos para el uso aceptable de los servicios tecnológicos y de los activos de información asociados del Instituto y deben propender por su confidencialidad, integridad y disponibilidad.

Lineamientos:

- No se permite en los equipos de cómputo y medios de almacenamiento propiedad de IDEAM, el almacenamiento de archivos de multimedia (audio, video, imágenes), programas ejecutables, o cualquier tipo de archivo que no sea de carácter institucional.

- Únicamente se permitirá el acceso a las aplicaciones y sistemas de información autorizados por la entidad, de esta manera evitar la ejecución de software no licenciado el cual atente contra los derechos de autor y propiedad intelectual según como lo regula la ley.

- La oficina de informática deberá coordinar y revisar de forma periódica el estado de configuración de los servicios de tecnología, estaciones de trabajo verificando que únicamente se encuentren instaladas y configuradas las aplicaciones permitidas de la línea base de software de la entidad.

- Los dominios ideam.gov.co y siac.gov.co son los únicos medios autorizado para la gestión de correo electrónico institucional, es decir que no se permite emplear otros medios de comunicación distintos a los que la entidad suministra a los funcionarios para el ejercicio de sus funciones.
- Todos los funcionarios, contratistas y proveedores que son autorizados para acceder a los servicios tecnológicos de la entidad, son responsables de toda actividad que sea ejecutada con las credenciales y privilegios de acceso otorgados.

- Es obligación de todos los funcionarios y/o contratistas dar cumplimiento a la normativa legal vigente, en materia de delitos informáticos, así mismo evitar malas prácticas que comprometan la seguridad de la información de IDEAM.

- En caso de requerir la emisión masiva de algún mensaje de interés institucional para divulgación, deberá tramitarse a través del grupo de comunicaciones de la entidad o el medio autorizado para gestionar la actividad.

- Toda comunicación, documentos, correos electrónicos, videos, imágenes o boletines informativos de interés institucional deberán cumplir con los estándares y/o formatos e imagen corporativa autorizada.

5.5.3. DEVOLUCIÓN DE ACTIVOS

Propósito: Los funcionarios, contratista y/o partes externas deberán realizar la devolución de todos los activos de información de la entidad que se encuentren a su cargo, al terminar su vinculación laboral, contractual entre otros.

Lineamientos:

- En los procesos de supervisión de contratos una vez finalizados según aplique el caso (terminaciones, finalización) se deberá formalizar o certificar la devolución de todos los activos de información físicos y/o electrónicos entregados, generados y procesados, los cuales son propiedad de la entidad.

- Para el caso de los equipos de cómputo propiedad del IDEAM asignados a contratistas y/o proveedores, deberán ser devueltos de manera formal como lo indica el proceso de entrega de cargo, adicionalmente contemplar la generación del respaldo de información el cual deberá ser solicitado por el jefe inmediato del funcionario, esta solicitud deberá estar soportada a través de la mesa de servicio.

5.5.4. CLASIFICACIÓN DE LA INFORMACIÓN

Objetivo: Asegurar que la información propiedad de IDEAM, dispone de un nivel apropiado de protección, de acuerdo con su criticidad e importancia para la entidad.

Lineamientos:

- La clasificación se debería incluir en los procesos de la organización, y debería ser consistente y coherente en toda la entidad.

- La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

- Cada área, grupo y/o dependencia al interior del IDEAM, será la encargada de clasificar los activos de información teniendo en cuenta los aspectos de

confidencialidad, disponibilidad, integridad de la información y el perjuicio que implicaría para la entidad en caso de presentarse daños, esto con el fin de desarrollar e implementar controles preventivos para preservar y custodiar adecuadamente los activos de información.

- Las oficinas de Gestión Documental y Asesora de Planeación, a través del sistema de gestión de calidad y el oficial de seguridad de la información definirán los lineamientos para la clasificación de la información teniendo en cuenta los requisitos legales y normativos vigentes (Las Tablas de Retención Documental (TRD) para indicar el tipo de clasificación de las series, subseries y documentos en ella contenidas), así mismo lo dispuesto en la ley 1712 de 2014.

- Toda comunicación, documentos, formatos institucionales deberán estar rotulados indicando el nivel de clasificación de la documentación acorde con los lineamientos establecidos en la guía de etiquetado de información.
- Para el intercambio de información se deberá tener en cuenta el nivel de clasificación y los términos de confidencialidad.

5.6. MANEJO DE MEDIOS

Objetivo: Establecer lineamientos para evitar la divulgación, modificación, destrucción y/o retiro no autorizado de la información almacenada en los diferentes medios.

Lineamientos:

- Todo equipo de cómputo que esté o requiera ser conectado a la red tecnológica del Instituto, debe estar acorde con los procedimientos de instalación definidos desde la Oficina de informática, donde se mantiene un registro de todos los equipos con acceso a los servicios de TI.

- Los líderes de las Subdirecciones, Oficinas y/o dependencias, conjuntamente con la Oficina de informática apoyarán el cumplimiento de las normas de instalación y notificaciones correspondientes de actualización, reubicación y/o reasignación de los equipos informáticos que den lugar.

- El mantenimiento preventivo y correctivo de la infraestructura tecnológica de IDEAM, será solicitado por el jefe de la Oficina de informática al coordinador del Grupo de Tecnología y Comunicaciones de dicha dependencia, quien deberá diligenciar el formato o cronograma E-GI-F038 FORMATO MANTENIMIENTO INFRAESTRUCTURA TECNOLOGICA v1 el cual es obligatorio realizarse para cada vigencia incluso cada vez que se deba actualizar, esto en cumplimiento de la implementación del plan E-GI-PL001 PLAN DE MANTENIMIENTO DE LOS SERVICIOS TECNOLÓGICOS v1.

- La Oficina de informática delegará el personal autorizado para tener acceso a los equipos de cómputo y poder brindar los servicios de mantenimiento y soporte informático, excepto de los equipos de cómputo que no son propiedad de la entidad.

5.6.1.1. GESTIÓN DE MEDIOS REMOVIBLES

Objetivo: Definir procedimientos para la gestión de medios removibles, de acuerdo con los lineamientos y esquemas de clasificación de la entidad

Lineamientos:

- El proceso de backup de información (en cintas) debe contar con las condiciones mínimas que permitan asegurar la confidencialidad, integridad y disponibilidad de la información en custodia.

- Los medios y equipos donde se almacena y procesa información, deben mantenerse con las medidas de protección físicas, lógicas y condiciones dadas por los fabricantes, que permitan un adecuado funcionamiento.

- Se restringe la copia de información institucional en medios removibles de almacenamiento no autorizados, para lo cual se limitará la funcionalidad en los equipos de cómputo, la autorización deberá tramitarse según las indicaciones dadas por la oficina de informática.

- El uso de medios removibles será restringido. En caso de requerir su uso deberá ser solicitado por la parte interesada de manera formal a través de la

mesa de servicio, posteriormente autorizado por la oficina de informática teniendo en cuenta lo siguiente:

- Definir en qué condiciones o casos se permitirá el uso (procedimiento guía o instructivo).

- La Oficina de informática deberá mantener un registro de los dispositivos y/o medios removibles autorizados.

- En caso de transferencia de información institucional se dispondrá de los repositorios comunes para el intercambio de información

- Realizar cambios periódicos de las contraseñas de cifrado de información.

- El uso de medios removibles deberá emplear métodos para el cifrado de información, para ello la oficina de informática deberá indicar los medios de cifrado, esto con el fin de evitar la pérdida y fuga de información institucional de carácter clasificada o reservada.

- Se deberá realizar un escaneo por medio de una herramienta de gestión de seguridad, cada vez que haga la conexión de un medio removible, igualmente no se permite la ejecución de programas y/o aplicación no autorizadas almacenadas en estos medios removibles.

5.6.1.2. DISPOSICIÓN DE LOS MEDIOS

Objetivo: asegurar adecuadamente la disposición de medios, para evitar la pérdida, fuga de información.

- Los medios que requieran ser eliminados, dar de baja o ser reasignados deberán ser sometidos a un proceso de borrado seguro y demás mecanismos que puedan considerarse, con el fin de evitar la recuperación de la información que alguna vez estuvo contenida en estos medios.

- En caso excepcional y justificado deberá realizarse un respaldo de información.

- Para esta actividad se debe gestionar un catálogo o inventario de los medios removibles donde se especifique su estado como Eliminado, Reasignado, Asignado según el caso.

- Deberá establecer los lineamientos donde se defina la disposición final de los desechos electrónicos.

- Se debe disponer de forma segura los medios de soporte cuando estos ya no se requieran, utilizando procedimientos formales.

5.6.1.3. TRANSFERENCIA DE MEDIOS FÍSICOS

- Toda información propiedad del IDEAM de tipo clasificada y/o reservada, almacenada en los diferentes medios y que requieran ser transportados a otras locaciones ajenas a la entidad, deberá cumplir con los lineamientos de seguridad establecidos por la oficina de informática.

- El transporte de medios de almacenamiento físico deberá ser llevado a cabo teniendo en cuenta las medidas preventivas mínimas de seguridad, necesarias para asegurar que el proceso de transporte de los medios de almacenamiento sea transportado de forma segura.

5.7. CONTROL DE ACCESO

5.7.1.1. REQUISITOS DE LA ENTIDAD PARA CONTROL DE ACCESO

Objetivo: establecer lineamientos para el acceso controlado a la información institucional, las instalaciones de procesamiento de información y servicios de TI.

Lineamientos:

- La gestión de accesos a la información digital y recursos de TI por parte de los usuarios deberá ser otorgado por la oficina de informática, mediante la asignación de credenciales de acceso (Usuario y contraseña) para los servicios a los que han sido autorizados y demás requeridos para el desempeño de sus funciones laborales.

- Los dueños de los activos de información deberán definir los privilegios de acceso adecuados, restricciones y especificación de los roles de los usuarios en relación a los accesos a la información.

- Las credenciales de acceso a los sistemas de información y recursos de TI, son de carácter personal e intransferible, por tal razón su uso será responsabilidad del funcionario, contratista y/o proveedores a los que se les ha realizado formalmente la asignación.

- Toda labor o actividad que se requiera ejecutar y acceder a los servidores, equipos o infraestructura de TI de IDEAM, deberá realizarse en las instalaciones, por tal motivo se restringe la ejecución de actividades de forma remota, sin la autorización previa de la oficina de informática.

- Las conexiones remotas a los servicios de TI institucionales, deberá realizarse a través de conexión por VPN con las directrices dadas por la oficina de informática, esta deberá ser autorizada y gestionada como lo indican los procedimientos.

    - Para gestión y control es necesario que el grupo de Tecnología y comunicaciones construyan e implementen un catálogo o inventario de asignación de VPN con atributos que permitan su control y faciliten la trazabilidad de hallazgos, ataques o intentos de fraudes

- La oficina de Informática deberá establecer una segmentación y/o segregación de las redes de comunicación, esto con el fin de aislar o separar los entornos de red de usuarios a los de red de servicios y demás recursos de TI.

    - Para gestión y control es necesario que el grupo de Tecnología y comunicaciones construya e implementen un catálogo de la segmentación de redes con atributos que definan su objetivo, los equipos que se encuentran en cada segmento, nombre del segmento,

fecha de creación, fecha de eliminación, fecha de modificación, entre otros.

- La oficina de informática a través de sus grupos de Tecnología y Comunicaciones y Sistemas de Información, con el apoyo del oficial de Seguridad del grupo de Arquitectura Empresarial y Seguridad de Información , será la encargada de liderar y coordinar la inspección y revisión de los controles de acceso a los sistemas de información y recursos otorgados a los diferentes usuarios y terceras partes de IDEAM, con el fin de verificar que únicamente tengan los accesos y privilegios autorizados a los diferentes servicios de Información.

    - Los Grupos de Tecnología y comunicaciones y Sistemas de Información deben construir, implementar y mantener un catálogo de los controles de acceso a los sistemas de información y recursos otorgados a los diferentes usuarios y terceras partes, dichos grupos deben ser los responsables de la gestión de dicho catálogo.

5.7.1.2. GESTIÓN DE ACCESO DE USUARIOS

Objetivo: Establecer mecanismos y lineamientos para el control de acceso a los servicios tecnológicos de la entidad y la prevención de los accesos no autorizados.

Lineamientos:

- La oficina de informática definirá un procedimiento formal para el acceso a los servicios de TI institucionales, así mismo los lineamientos para la creación de cuentas de usuario del dominio ideam.gov.co.

- La oficina de informática deberá Mantener y custodiar un inventario actualizado de cuentas de directorio activo.

- La generación de contraseñas de acceso deberá cumplir con las características mínimas, bien sea cuentas de usuario estándar, administradores, entre otros.

- Implementar el principio de mínimo privilegio en los recursos a los que se accederá en carpetas corporativas o drive institucional con el fin de garantizar que ante un acceso no autorizado, no pueda acceder a recursos y/o información que no es necesaria para ese usuario

- En ninguna circunstancia se permitirá conservar configuraciones de acceso estándar, una vez generadas o asignadas deberán cambiarse para evitar intrusiones a los sistemas de información.

- No se permitirá el acceso compartido a los diferentes servicios de información, en caso de requerir accesos privilegiados deberán ser solicitados y aprobados por la oficina de informática, a través del Grupo de Tecnología y Comunicaciones.

- El usuario asignado por directorio activo en lo posible deberá poder integrarse e interoperar con otros servicios a través del directorio activo.

- Los accesos a los servicios de tecnología únicamente serán otorgados tal como lo indica los lineamientos para la gestión de accesos a servicios de TI y aquellos que sean solicitados y autorizados por el jefe inmediato y/o supervisor de contrato.

- Las conexiones remotas para la administración de la plataforma de TI deberán restringirse, únicamente se permitirá el acceso a personal autorizado por la oficina de informática.

- Verificar la desactivación o modificación de cuentas de usuario teniendo en razón a situaciones administrativas como: vacaciones, licencias no remuneradas, desvinculación, entre otras, en dado caso que se presente inactividad en la cuenta de usuario superior a ocho (8) días esta será deshabilitada.

- Todo aplicativo o software deberá ser adquirido y aprobado por las áreas encargadas, e informar a la Oficina de informática dentro del término de un periodo de tiempo no menor a quince (15) días, previo a su entrega formal a

dicha dependencia para su puesta en producción o instalación, aclarando el objetivo de uso de dicho software, el dueño del mismo, su número de inventario, su proveedor, entre otros, para tener el control sobre este elemento, lo anterior dando cumplimiento al procedimiento de adquisición de bienes y servicios de IDEAM.

- Las credenciales de acceso de usuarios que tengan rol super - administrador, deberán dejarse en custodia en sobre sellado como lo determina el proceso administración de claves sensibles; estas credenciales deberán ser modificadas de forma periódica o cuando el administrador o jefe inmediato lo determinen.

    - Dichas credenciales deberán ser entregadas al oficial de Seguridad como se indicó anteriormente dejando una copia de las mismas en documento físico en propiedad de quien las entrega. En caso de pérdida de las claves por parte de quien la entrega deberá realizar la modificación de inmediato de las mismas y realizar nuevamente la solicitud formal de entrega y avisar oportunamente el cambio de las mismas.

- El sistema de autenticación de usuarios deberá parametrizar un proceso de expiración de contraseñas cada sesenta (60) días, igualmente deberá mantener un registro de las 5 últimas contraseñas empleadas por usuario y así evitar la reutilización de éstas.

- Reportar oportunamente a la oficina de informática por intermedio de la mesa de servicios al Oficial de Seguridad, sobre cualquier incidencia o eventualidad donde se tenga sospecha que otra persona esté utilizando el usuario y roles asignados o se evidencien comportamientos inusuales.

- Es responsabilidad de los líderes de proceso, jefe de oficina, subdirector o jefe inmediato reportar a la oficina de informática las novedades de personal según sea el caso, a través de la mesa de servicios de IDEAM, con un intervalo de tiempo no inferior a cinco (5) días calendario.

- La inactivación, modificación y retiro de los privilegios de acceso deberán formalizarse mediante una solicitud a través de la mesa de servicios y ser remitida por los jefes de oficina, subdirectores o coordinadores de grupo de las dependencias", la cual deberá ser atendida de forma inmediata.

5.7.1.3. RESPONSABILIDADES DE LOS USUARIOS.

Objetivo: Definir lineamientos para que los usuarios den cumplimiento a las buenas prácticas de la entidad en lo referente al uso de información secreta para la autenticación.

Lineamientos:

- Las credenciales de acceso son de carácter personal e intransferible. El cambio de contraseña podrá ser solicitado por el titular de la cuenta y los cambios pueden realizarse cuando se considere pertinente en el marco del cumplimiento de la política de expiración de contraseñas definidas en el directorio activo.

    - Validar la autenticidad del usuario para gestionar la solicitud.

- La generación de contraseñas debe contener cierto grado de complejidad, por tal razón no se recomienda que contengan palabras comunes, o algún dato referente al titular de la cuenta de usuario ejemplo, fechas de acontecimientos, nombres familiares, números de identificación entre otros.

  La generación de contraseñas de acceso deberá cumplir con los siguientes parámetros:

    - Tener mínimo 8 caracteres
    - Caracteres en mayúsculas
    - Caracteres en minúsculas
    - Contener dígitos numéricos (0 a 9)
    - Contener caracteres especiales (@+*/&%$#)

- Bajo ningún caso se deberá dar a conocer o divulgar las contraseñas, en caso de solicitar acceso con la cuenta del titular el proceso deberá formalizarse con el jefe inmediato, tampoco se permite mantener anotadas las contraseñas en papel a libre exposición.

- Una vez asignado los accesos a la plataforma tecnológica, en su primer inicio de sesión deberán cambiarse las contraseñas suministradas por la mesa de servicio.

- La oficina de informática deberá parametrizar en los sistemas de autenticación de usuario, el bloqueo de cuentas de usuario de forma inmediata después de ingresar 4 intentos fallidos de ingreso de contraseñas.

- Una vez realizado el bloqueo el usuario deberá esperar un tiempo prologando de 15 minutos para volver a intentar el inicio de sesión, en dado caso de presentar dificultad para restablecer el acceso podrá acudir por medio de una solicitud a la mesa de servicios de IDEAM.

- No enviar archivos con datos de la organización y/o entidad, por medios no oficiales como whatsapp, dropbox, wetransfer, correos no oficiales, entre otros.

- Evitar la instalación de programas o extensiones de navegadores de fuentes desconocidas ya que estas pueden traer malware (software malintencionado) que puede afectar la integridad de los dispositivos y exponer la información sensible no solo propia, sino de las redes a las que se conectan

- Cuando se usen aplicaciones de mensajería instantánea estas deben garantizar el uso de encriptación extremo a extremo *(end-to-end)* y que tenga una política de privacidad y tratamiento de datos aceptable

5.7.1.4. CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

Objetivo: Definir mecanismos para evitar el acceso no autorizado a sistemas, aplicaciones y servicios de tecnología.

Lineamientos:

- La oficina de informática deberá establecer mecanismos que permitan controlar el acceso a los ambientes de desarrollo, pruebas, producción y la separación de estos, así mismo limitar y controlar el acceso a terceras partes (contratistas y proveedores).

- Las sesiones de usuario iniciadas en los aplicativos institucionales, después de registrar inactividad, deben cerrarse de forma controlada e implementar mecanismos de seguridad al intentar restablecer la conexión.

- Las sesiones en aplicativos web deben ser invalidadas en un tiempo no mayor a 24 horas después del inicio de sesión.

Activar factores múltiples de autenticación (MFA) en las cuentas de correo y otros sistemas, con el fin de confirmar la identidad del que accede al servicio y demás herramientas asociadas, en la medida de lo posible no debe tener la validación de la identidad por vía SMS.

- La entidad en coordinación con la oficina de Informática deberá establecer controles que permitan integrar la autenticación de los sistemas de información con directorio activo, en caso de usuarios externos deberá disponer con un registro de inventario, actualizado, además de la formalización y asignación de cuentas de usuario a los diferentes sistemas de información.

- Las contraseñas locales, encriptadas de manera irreversible, deben usarse como respaldo de último recurso si el servidor TACACS, DIAMETER u otro, no funciona o no es accesible.

- La oficina de Informática deberá implementar controles para que los usuarios de los diferentes recursos de la plataforma tecnológica no puedan instalar y/o ejecutar software o aplicaciones que permitan evadir controles de seguridad, en caso de requerir el uso de aplicaciones que no son parte de la línea base de software de IDEAM, deberán realizar una solicitud indicando la necesidad o justificación del uso formal, a la oficina de informática la cual emitirá un concepto técnico y notificará la respuesta a la solicitud.

    - En caso de identificar algún programa o aplicación no autorizada por la oficina de informática deberá ser desinstalada y eliminada inmediatamente.

- Para el acceso a los sistemas de información, es necesario que en el proceso de autenticación de usuario no permita visualizar las contraseñas digitadas,

igualmente deshabilitar y no permitir el recordatorio de las credenciales de acceso e inicios de sesión automática.

- Emplear mecanismos de seguridad como el bloqueo de sesión después de tres (3) intentos de ingreso erróneo, así mismos controles para el restablecimiento del acceso mediante la validación de la autenticidad del usuario y la generación de contraseñas temporales, las cuales deberán ser modificadas después de su primer uso.

- Definir e implementar procedimientos seguros para los sistemas de información y aplicaciones de IDEAM, Fortalecer los controles de autenticación de usuarios, en los diferentes sistemas de información.

- Que permita ejercer control de auditoría sobre los sistemas de información en los diferentes privilegios de usuario.

- Limitar los accesos al código fuente de los sistemas de información, este acceso únicamente estará permitido a los usuarios con los privilegios asignados (desarrollo y soporte) y aquellos autorizados por la oficina de informática.

5.8. CRIPTOGRAFÍA

Objetivo: Definir lineamientos para el uso apropiado y eficaz de controles criptográficos para asegurar la confidencialidad, integridad y autenticidad de la información institucional.

Lineamientos:

- La oficina de informática deberá definir los lineamientos y disponer de los medios para realizar el cifrado de información que es transportada y/o almacenada en dispositivos móviles y medios removibles.
-
- Todos los sitios web que procesen información deben contar con capa de conexión segura *(Secure Sockets Layer- SSL)*. Así mismo, ninguna contraseña debe ser almacenada en texto plano y se debe implementar un proceso de cambio de contraseñas periódico.

- Los métodos de cifrado de información serán aplicados teniendo en cuenta los siguientes casos que deben ser aplicados.

    - Protección de contraseñas de acceso a servicios de información, administración de plataforma de TI entre otros.
    - Transferencia de información digital de carácter clasificada o reservada.
    - Procesos de generación y transporte de copias de seguridad.
    - Conexión y disposición de canales de comunicación con otras entidades públicas y/o privadas.

- Mantener y actualizar un inventario de los sistemas de información que requieran implementar controles criptográficos de acuerdo con la criticidad de la información almacenada.

- Para todos los sistemas de Información del IDEAM, las credenciales de acceso deben ser almacenados en archivos o tablas de bases de datos con cifrado de información.

- Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.

5.9. SEGURIDAD FÍSICA Y DEL ENTORNO

5.9.1.1. ÁREAS SEGURAS

Objetivo: establecer lineamientos para prevenir el acceso físico no autorizado, el daño y la interferencia a la información y las áreas e instalaciones de procesamiento crítico de información de la Entidad.

Lineamientos:

- El Proceso de gestión de servicios administrativos a través del grupo de servicios administrativos, deberá señalizar y demarcar las áreas seguras.

- Para las áreas seguras será necesario implementar controles de acceso físico bien para prevenir accesos no autorizados, además de esto deberán

permanecer cerradas con llave, en el momento que no haya supervisión del funcionario responsable o estas se encuentren desocupadas.

- Los puntos de acceso físico a la entidad deberán estar supervisados mediante Cámaras de Circuito Cerrado de Televisión CCTV, además de disponer de un área de recepción con vigilancia que permita controlar el acceso a las instalaciones de la entidad.

    - El acceso a los sitios e instalaciones debería estar restringido únicamente para personal autorizado;

- La seguridad perimetral de las instalaciones físicas, áreas seguras y áreas de procesamiento crítico de información, deberá disponer de controles de seguridad como CCTV, alarmas de detección de intrusos, las cuales deberán ser monitoreadas por el personal de seguridad de IDEAM.

- El grupo de servicios administrativos deberá definir e implementar controles de acceso físico a la entidad, así mismo supervisar el acceso a las áreas seguras y áreas de procesamiento crítico de información.

5.9.1.2. CONTROLES DE ACCESO FÍSICOS

Objetivo: Definir lineamientos para evitar accesos no autorizados a las instalaciones y/o áreas de procesamiento de información, que afecten la confidencialidad, integridad y disponibilidad de la información de la entidad.

Lineamientos:

- La entidad deberá implementar y mantener un registro íntegro y actualizado que permita verificar la fecha y hora de ingreso / salida de personal tanto para funcionarios, contratistas y visitantes de IDEAM.

- Los accesos de visitantes deberán ser autorizados por algún funcionario y su ingreso a las instalaciones deberá ser supervisado. Los accesos únicamente

serán autorizados con propósitos específicos, igualmente también se deben mantener registros en una bitácora de acceso para visitantes.

  - Los visitantes durante su permanencia en las instalaciones deberán permanecer acompañados por parte de algún funcionario de la entidad.

- Es obligación que todos los funcionarios, contratistas y visitantes, portar el carnet o la tarjeta de identificación de visitantes en un lugar visible durante su permanencia en las instalaciones de la Entidad.

- El personal de vigilancia deberá mantener un registro o el diligenciamiento de una bitácora y/o sistema de información para el ingreso y salida de elementos de tecnología (equipos de cómputo, Tablet, discos duros, cámaras de video, dispositivos de red, entre otros)

  - En caso de requerir la salida de elementos de TI los cuales sean propiedad del IDEAM, se deberá contar previamente con autorización expresa de la oficina de informática y el grupo de servicios administrativos según sea el caso y de acuerdo con los procedimientos establecidos para tal fin.

- El personal de vigilancia deberá establecer mecanismos para inspeccionar el ingreso y salida de bolsas, morrales, maletines, cajas entre otros, para evitar la sustracción no controlada de información y elementos de tecnología de la Entidad.

- La oficina de Informática, deberá controlar el ingreso y salida a los centros de datos y centros de cableado así mismo registrar y verificar el Ingreso y salida de elementos de tecnología de estas áreas, igualmente en caso de requerir acceso por parte de personal ajeno a la entidad, este deberá estar supervisado y acompañado por quien sea autorizado, éste se hará responsable de la estadía durante el tiempo de permanencia en las instalaciones.

- La entidad deberá diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes así mismo implementar controles

que permitan evitar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles o causados por el hombre.

- Se debe restringir el uso de equipo fotográfico, video, audio u otros elementos de grabación dentro de las áreas seguras y de procesamiento crítico de información sin la debida autorización.

- El proceso de Servicios administrativos a través del grupo de recursos físicos, deberá revisar y supervisar el proceso de respaldo de las grabaciones generadas por las cámaras de vigilancia, igualmente para la información generada y registrada en el proceso de acceso físico a las instalaciones de la entidad.

- El proceso de Servicios Administrativos y Gestión Financiera, deberán establecer controles para el acceso a las áreas destinadas para el proceso de pagos, además estas deberán estar vigiladas y monitoreadas mediante cámaras de CCTV y controles establecidos según la guía de seguridad para el Manejo y Control de Recursos Financieros de MinTIC.

- El trabajo en áreas seguras debe estar vigilado o supervisado por cámaras de CCTV, para ello las cámaras no podrán estar enfocadas directamente a la captura de información dentro de estas áreas.

- No se permite el consumo de alimentos y bebidas en las áreas seguras y áreas de procesamiento crítico de información, esta restricción debe ser informada y señalizada.

5.9.1.3. ÁREAS DE DESPACHO Y CARGA

Objetivo: controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos con el fin de evitar accesos no autorizados.

Lineamientos:

- El Grupo de Servicios Administrativos deberá identificar las áreas de cargue y descargue, estas deberán ser demarcadas, controladas y vigiladas mediante controles de cámaras de CCTV

- El acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado

- En la operación del proceso las partes interesadas deberán realizar inspección de los elementos que ingresan y salen por las áreas de cargue y descargue.

- El proceso también deberá ser supervisado y registrado en las bitácoras de vigilancia.

5.10. EQUIPOS

Objetivo: Definir lineamiento para prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

Lineamientos:

- El Proceso de servicios administrativos y la oficina de informática a través del grupo de Tecnología y Comunicaciones, deberán dar las directrices para la adecuada ubicación y protección de los equipos de cómputo e impresoras, deben estar ubicados, protegidos contra amenazas ambientales y acciones no autorizadas.

    - Los equipos de cómputo portátiles propiedad de la entidad deberán protegerse mediante mecanismos que prevengan la pérdida de estos.

- La entidad deberá Controlar y supervisar el uso de las conexiones eléctricas, para el uso de la energía regulada en las áreas de trabajo, únicamente se deben conectar equipos de cómputo bien sea de escritorio o portátiles, pantallas, los otros elementos deberán hacer uso de la red eléctrica no regulada.

- Hacer uso de herramientas de protección del dispositivo como EDR (Endpoint Detection and Response), solución de protección de malware avanzado, los cuales permiten una gestión integral y centralizada de las diferentes amenazas cibernéticas y de la política de seguridad de la empresa de manera local para el control en los dispositivos de los empleados

- Para asegurar la operación de la infraestructura tecnológica de IDEAM, ante posibles fallos en el suministro eléctrico, se deberán definir e implementar estrategias de suministro eléctrico alterno como plantas eléctricas y/o UPS, que permitan mitigar daños directos a la infraestructura de TI y como aseguramiento a las operaciones de la entidad.

    - Para las plantas eléctricas y UPS, deberán coordinarse y ejecutarse los respectivos mantenimientos preventivos y correctivos programados en el cronograma del Plan de mantenimiento de servicios Tecnológicos.

- El grupo de servicios administrativos, deberá verificar y proteger el cableado en las instalaciones, para los servicios de voz, datos y energía, contra la interferencia o daños locativos que afecten la prestación de estos.

    - El cableado eléctrico deberá estar separado del cableado del servicio de comunicaciones.

- Los centros de datos y cuartos de cableado deberán permanecer libres de objetos y/o elementos ajenos a la operación de TI.

5.10.1.1. MANTENIMIENTO DE EQUIPOS

Objetivo: Definir lineamientos para asegurar la disponibilidad de los servicios tecnológicos y la adecuada gestión de mantenimiento a los componentes de TI.

Lineamientos:

- La oficina de informática deberá hacer revisión de los componentes de la infraestructura de TI y seguimiento de las condiciones técnicas sugeridas por los fabricantes para su adecuada operación teniendo en cuenta los aspectos ambientales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente la operación de las instalaciones de procesamiento de información.

- La oficina de informática deberá definir, ejecutar y formalizar un proceso para el mantenimiento de la infraestructura tecnológica de la Entidad.

  - Se debe mantener un cronograma oficial de los mantenimientos preventivos, el cronograma de contemplar toda la infraestructura tecnológica de IDEAM y el tiempo de ejecución de los mismos, así mismo deberá ser actualizado para cada vigencia el cronograma oficial para el mantenimiento preventivo como lo estipula el plan de mantenimiento de servicios tecnológicos.

  - Los procesos de mantenimiento preventivo o correctivo únicamente podrán ser ejecutado por el personal designado y autorizado.

  - El proceso de mantenimiento deberá ser coordinado y aprobado por las diferentes partes interesadas en caso de que estas actividades puedan generar una suspensión parcial del servicio

  - Los equipos de cómputo, redes y comunicaciones suministrados por IDEAM no deben alterarse de ninguna manera ni realizar cambios en la configuración ni adición de componentes, sin el consentimiento y autorización de la oficina de informática.

  - La Oficina de informática a través del Grupo de Tecnología y Comunicaciones, deben realizar copias de respaldo de la información de los equipos de cómputo, configuración de routers, servidores, activos de red, y en general de la infraestructura tecnológica de IDEAM previamente a la realización de mantenimientos preventivos y correctivos programados como lo estipula el plan de Mantenimiento de Servicios tecnológicos.

  - Para los servicios en mantenimiento la oficina de informática y las partes interesadas evaluarán si se requiere la activación del plan de recuperación de desastres, en el marco de la ejecución de mantenimiento preventivo y/o correctivo de los servicios tecnológicos de IDEAM.

5.10.1.2. RETIRO DE ACTIVOS

Objetivo: Definir lineamientos para controlar la adecuada gestión y uso de medios tecnológicos fuera de las instalaciones de IDEAM, asegurando la confidencialidad de la información.

Lineamientos:

- La salida de elementos de tecnología deberá ser autorizada como lo indican los procedimientos para este fin y deberá ser supervisada y registrada por el personal de vigilancia, además de esto tener en cuenta lo siguiente:
    - Verificar la criticidad de la información contenida en estos medios, de ser clasificada deberá disponer de un respaldo de información en caso perdida.
    - Para la información reservada evaluar la debida autorización y métodos adicionales que permitan proteger la información (cifrado de datos)

- Para los funcionarios que en ejercicio de sus funciones deban realizar desplazamiento a otras ciudades, los equipos portátiles se deben llevar como equipaje de mano para evitar daños físicos o pérdida de los mismos.

- Los equipos tecnológicos retirados de las instalaciones de IDEAM, no se deberían dejar sin vigilancia en lugares públicos.

5.10.1.3. DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS.

Objetivo: Definir lineamientos para la adecuada gestión de medios para asegurar que cualquier dato sensible o software licenciado haya sido retirado o sobre escrito en forma segura antes de su disposición o reúso.

Lineamientos:

- Los equipos de cómputo propiedad del IDEAM, los cuales requieren ser asignados o dados de baja, deberán ser sometidos a un proceso de borrado

seguro y respaldo de información con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

5.10.1.4. EQUIPOS DE USUARIO DESATENDIDOS Y POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.

Objetivo: Brindar lineamientos para la protección adecuada a los equipos desatendidos para evitar sabotajes internos, accesos no autorizados y pérdida de información.

Lineamientos:

- Todos los usuarios deben realizar el cierre de la sesión de dominio y sistemas de información cada vez que termine su jornada laboral o cuando se ausenten un tiempo muy prolongado de sus sitios de trabajo.

- Todos los usuarios deben bloquear su estación de trabajo cuando se ausenten de sus sitios de trabajo.

- La oficina de informática deberá parametrizar a través de las políticas de directorio activo un bloqueo de sesión una vez registrados 3 minutos de inactividad como medida preventiva, igualmente, que todos los equipos de cómputo que estén dentro del dominio de IDEAM, oculten los iconos y accesos directos a información que se encuentren en el escritorio.

- Se debe verificar que los equipos de cómputo y sesiones de usuario de los funcionarios que se encuentren ausentes bien sean vacaciones, licencias según sea el caso, se encuentren inactivos, en caso tal de existir algún reemplazo el usuario debe ingresar con sus credenciales propias de acceso.

- Toda información física y digital institucional deberá mantenerse debidamente custodiada y preservada en lugares seguros, se deberá evitar la exposición de información en las áreas de trabajo durante la ausencia del funcionario responsable.

- Para el proceso de impresión de documentos de información con altos niveles de confidencialidad, estos deberán ser retirados de forma inmediata de los dispositivos de impresión y tampoco deberán dejarse a libre exposición en áreas comunes o sitios de trabajo sin custodia por parte del colaborador.

- Es responsabilidad de todos los funcionarios, contratistas y/o proveedores dejar en orden su escritorio al final de cada jornada laboral para evitar la pérdida de documentos e información confidencial. Para tales efectos IDEAM provee escritorios, archivadores y demás medios.

- No se permite que los usuarios que tengan privilegios de impresión suministren o hagan préstamo de sus claves, pines y estaciones de trabajo para imprimir.

    - Es importante reiterar que todo privilegio de impresión es autorizado y controlado, para ello se realiza la asignación de un pin de impresión el cual es personal e intransferible.

- Toda la información física que no se requiera para ningún propósito, debe evaluar la criticidad de la información para desecharse de manera segura para tales efectos esta debe ser destruida en su totalidad asegurándose que no pueda ser reconstruida.

    - Para el caso de la reutilización de papel se debe verificar la información contenida en estos documentos, no se debe reutilizar información clasificada o reservada así mismo que contenga datos personales, los documentos reutilizables deberán demostrar total nulidad.

5.11. SEGURIDAD DE LAS OPERACIONES

5.11.1.1. PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS

Objetivo: Establecer lineamientos para el aseguramiento y disponibilidad de los recursos tecnológicos del IDEAM, mediante la documentación y estandarización de procesos de la Operación tecnológica.

Lineamientos:

- Se debe documentar los procedimientos operativos específicos de TI, los cuales deben ser documentos formales dentro del SGI acorde a los lineamientos de la guía de elaboración de documentos.

    - Estos documentos deberán ser aprobados, socializados y publicados.

- La oficina de Informática deberá poner a disposición de todos los colaboradores los procedimientos de operación de TI

- El plan de implementación para el uso de servicios de nube en la Entidad debe estar articulado al Diagnóstico del Modelo de Seguridad y Privacidad de la información, además de realizar las actualizaciones pertinentes en el Plan Estratégico de Tecnologías de la información PETI. Lo anterior para permitir dar cumplimiento al conjunto de normas que integran la política de gobierno digital, proferida por el Ministerio de Tecnologías de la Información y las Comunicaciones, y particularmente en lo que respecta a seguridad digital, cumplir con los lineamientos y estándares señalados en el habilitador de seguridad y privacidad

5.11.1.2. GESTIÓN DE CAMBIOS

Objetivo: Establecer lineamientos que permitan gestionar adecuadamente los cambios en los procesos y operaciones de TI, sistemas de procesamiento de información de la entidad, con el fin de reducir afectaciones que comprometan la disponibilidad, integridad y confidencialidad de la información.

Lineamientos:

- La oficina de informática deberá definir un proceso formal que permita gestionar los diferentes cambios a nivel de infraestructura tecnológica y demás componentes de la plataforma.

- El proceso de Gestión del Cambio deberá considerar lo siguiente:
- Establecer un comité de cambios como lo define el proceso de gestión de cambios E-GI-P014 PROCEDIMIENTO GESTION DE CAMBIOS y su RFC

asociado para evaluar, aprobar o cancelar la ejecución del cambio proyectado, este comité debe definir los diferentes roles.

- Proceso formal de solicitud y ejecución del cambio.
- Gestión de riesgos e impactos potenciales del cambio.
- Comunicación del cambio a las partes interesadas.
- Informe de resultados.

- El Oficial de Seguridad de la Información debe estar incluido en el proceso de control de cambios para asegurar que los cambios implementados no comprometen la seguridad de la Información.

5.11.1.3. GESTIÓN DE CAPACIDAD.

Objetivo: Asegurar que la capacidad y disposición de recursos de TI, sean adecuadas para el aseguramiento de la prestación de servicios críticos y el cumplimiento a los objetivos institucionales.

Lineamientos:

- La oficina de informática deberá documentar y actualizar la gestión de capacidad de la plataforma de TI, incluyendo los roles, responsables, que permita evaluar las necesidades de los componentes de tecnología en operación y proyección de requerimientos de capacidad.

- Los requisitos de capacidad se deberán identificar y priorizar teniendo en cuenta la criticidad que tiene para IDEAM el recurso de TI involucrado.

- La Oficina de Informática en el marco de la operación de los servicios tecnológicos deberá implementar y aplicar controles de detección que indiquen los problemas oportunamente.

  - Deberá documentar acciones de mejora, correspondiente al alcance de las funciones y responsabilidades de cada grupo de coordinación de la oficina de informática.
  - Gestionar indicadores de gestión de capacidad y disponibilidad, los cuales deberán ser ejecutados en la periodicidad que se programen acorde a su contexto de aplicación para lo cual serán responsables los grupos de coordinación de la oficina de informática si les compete.

- La gestión de capacidad también deberá considerar las proyecciones de los requisitos sobre la capacidad futura de nuevos servicios, sistemas de información que será proyectada por los grupos de tecnología y Comunicaciones y Sistemas de información de la oficina de informática de acuerdo con las necesidades reales manifestadas por los interesados o demás dependencias del IDEAM.

5.11.2. SEPARACIÓN DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y PRODUCCIÓN.

Objetivo: Definir lineamientos para controlar la operación y separación de los ambientes de desarrollo, pruebas y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.

Lineamientos:

- Los ambientes de desarrollo, pruebas y producción que disponga IDEAM, ya sea de desarrollo interno o contratado con terceras partes, deben estar separados física y lógicamente, para reducir los riesgos de accesos o cambios no autorizados a los sistemas en producción.

- La oficina de informática deberá verificar la asignación de roles y privilegios de acceso a estos ambientes, además de esto deberá incluir:

    - Procedimientos de retorno incluyendo responsabilidades para abortar y recuperarse de cambios no satisfactorios y eventos imprevistos.

    - Segregación de las funciones y responsabilidades del personal que, opere y en general mantenga y administre los diferentes ambientes.

- No se permite la ejecución de pruebas, instalaciones o desarrollos de software, directamente sobre el entorno o ambiente productivo. Esto puede conducir a posibles fraudes.

- Realizar un proceso de ofuscamiento para los datos empleados en el ambiente de pruebas, no se permite el uso de datos reales del ambiente productivo en el ambiente de pruebas.

- Los ambientes deben estar claramente identificados y documentados, para así poder evitar confusiones en la ejecución de tareas o en la ejecución de procesos propios de cada uno.

5.11.3. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Objetivo: Desarrollar estrategias para la protección de la información y componentes de la infraestructura de TI, contra códigos maliciosos.

Lineamientos:

- Se deberán implementar y documentar controles que permitan detectar, prevenir, mitigar y recuperar afectaciones potenciales generados por códigos maliciosos

  La oficina de informática a través de la gestión de seguridad de la información deberá desarrollar estrategias que permitan sensibilizar y orientar a los usuarios en lo referente a la prevención y protección contra códigos maliciosos.

- El protocolo simple de administración de red (SNMP) no debe usar comunidades predeterminadas. En general, el acceso SNMP debe restringirse a privilegios de solo lectura o utilizar autenticación. Las listas de acceso deben usarse para restringir las direcciones IP desde las cuales se pueden originar las solicitudes SNMP.

- Reforzar la cultura y el entrenamiento de políticas corporativas para el uso apropiado de los recursos (herramientas de teletrabajo, manejo de información, Redes Virtuales Privadas (VPN), e infraestructura tecnológica) y aplicación de la navegación en internet con criterio preventivo.

- Los equipos de cómputo de IDEAM, deberán disponer de un software de antivirus que permita proteger y prevenir incidencias por códigos maliciosos,

este software deberá mantenerse con licenciamiento vigente, actualizado y soportado.

- El Antivirus corporativo debe contar con un contrato de soporte adicional al contrato de compraventa por parte del proveedor, y este se debe renovar oportunamente.

- Es software de antivirus deberá revisarse que se encuentre instalado y habilitado en los equipos de cómputo de IDEAM.

- No se permite la desactivación del software de antivirus.

- Se debe restringir el uso, ejecución, descarga de aplicaciones no licenciadas y que no sean parte de la línea base de software de IDEAM

- La conexión de equipos de cómputo que no son propiedad de la entidad deberá ser autorizada y se deberá realizar un proceso de verificación de requisitos de seguridad definidos por la oficina de informática.

- La oficina de informática deberá coordinar, ejecutar revisiones e inspecciones para el uso de software malicioso en las estaciones de trabajo y servidores.

- La oficina de informática debe implementar controles que permitan analizar, detectar y restringir el uso de software malicioso que provenga de descargas de sitios web de baja reputación y / o procedencia desconocida.

- La Oficina de informática deberá coordinar y ejecutar un plan de aplicación de actualizaciones y parches de seguridad en los sistemas operativos y equipos de infraestructura tecnológica para la protección de código malicioso.

- Se deben mantener actualizados los sistemas operativos, navegadores, manejador de contenidos, librerías y todo el software, con los últimos parches de seguridad liberados por el fabricante conforme a las políticas establecidas por la entidad.

- Todo mensaje de correo electrónico de procedencia desconocida deberá reportarse de forma inmediata a la oficina de informática a través de la mesa de servicios.

5.12. COPIAS DE RESPALDO

Objetivo: Definir lineamientos y desarrollar estrategias para preservar la integridad y disponibilidad de la información y servicios de procesamiento de información para la protección contra la pérdida de datos.

Lineamientos:

- La oficina de informática deberá documentar un plan para generación de copias de respaldo de información teniendo en cuenta lo siguiente:
    - Se debe definir y documentar un esquema de respaldo de la información.
    - La generación de copias de seguridad y respaldo de información deberá solicitarse formalmente a través de la mesa de servicios y la debida autorización de la oficina de informática.
    - Las copias de respaldo de la información y sistemas de información críticos para la entidad deben ser programadas y ejecutadas de acuerdo con las necesidades del Instituto, las características de los respaldos de información deben ser definidas por el propietario de la información según los requerimientos del mismo.
    - **Frecuencia del respaldo:** El IDEAM debe seguir un procedimiento definido de actividades de backup, teniendo en cuenta la criticidad y las necesidades de disponibilidad de los datos respaldados, en este procedimiento debe especificar al detalle, qué información será respaldada y los tiempos de ejecución ya sea diaria, semanal, mensual, semestral o anualmente.
    - **Almacenamiento de las copias de Respaldo**. La Entidad deberá proporcionar los medios necesarios para asegurar el proceso de almacenamiento.

- La oficina de informática mantendrá los periodos de retención de información que se encuentra respaldado acorde a las tablas de retención documental dictadas por el archivo general de nación y aquellas definidas por cada dependencia.

- **Seguridad del almacenamiento**. El lugar de alojamiento de las copias de seguridad y respaldo de información debe tener un adecuado nivel de protección física, ambiental y lógica, así mismo las condiciones de seguridad para soluciones cloud de IDEAM.

- **Restauración y pruebas**. El proceso de restauración y respaldo debe ser regularmente verificado para evaluar su efectividad ensayando su oportuna restauración, registrando eventos y posibles fallas.

- La oficina de informática deberá tener un inventario y/o bitácora de registro de copias seguridad realizadas y de las copias de respaldo restauradas.

    - Esta bitácora o inventarios deben ser expuesto y justificados con periodicidad quincenal al jefe de la oficina de Informática y al oficial de Seguridad de Información.

- Todo funcionario de cada área del IDEAM es el responsable de realizar copias de la información crítica y esencial para la normal ejecución de sus funciones y deberá copiarla en los medios de almacenamiento compartido que para tal objetivo a dispuesto la Oficina de informática para que esta dependencia realice las copias de seguridad de acuerdo con lo contemplado en la Política de Confianza y Seguridad Digital. Toda información que se aloje en los equipos propiedad del IDEAM y que se encuentran asignados a cada funcionario del IDEAM será responsabilidad de este y no de la Oficina de informática.

- La oficina de Informática suministrará los medios de almacenamiento compartido y propenderá por la disponibilidad del servicio, es responsabilidad del propietario de la información mantener la confidencialidad y otorgar privilegios de acceso a los repositorios de almacenamiento.

- No se permite que los usuarios realicen copias de seguridad de información institucional en medios extraíbles de información, en caso de requerir un respaldo este deberá ser solicitado de manera formal a la oficina de informática.

5.13. REGISTRO (LOGGING) Y SEGUIMIENTO

Objetivo: Definir lineamientos que permitan asegurar el registro de eventos y generación de evidencias en las operaciones de los servicios tecnológicos.

Lineamientos:

- La oficina de informática deberá generar registros de auditoría (logs) que permitan verificar y revisar eventos que puedan comprometer la seguridad de la información en los servicios de tecnología y sistemas de información.
    - La información contenida en los logs se debe proteger contra intentos de alteración y acceso no autorizado conservando integridad.
- La generación de registros de auditoría debe contribuir con la protección contra cambios no autorizados y errores operacionales.
- Los registros de auditoría deben ser custodiados y retenidos por el tiempo que el IDEAM lo determine. Según sea el caso, se debe hacer copia de respaldo de información de los registros de auditoría, ya que en caso de un incidente de seguridad de la información estos deberán estar disponibles.
- La oficina de informática debe implementar y documentar controles que permitan monitorear la operación, disponibilidad y capacidad de la infraestructura tecnológica
- La oficina de informática debe sincronizar los relojes de los servidores y demás componentes de la plataforma tecnológica, con una fuente única de referencia de tiempo con la hora legal colombiana http://horalegal.inm.gov.co/.
    - Esta sincronización permitirá evidenciar con exactitud los registros de auditoria.

- Esta sincronización se debe presentar mediante informe con evidencias al jefe de la oficina de informática, a los coordinadores de los grupos y al oficial de Seguridad de dicha dependencia. Además, se debe monitorear los relojes de todos los servidores con una periodicidad semanal y ajustarlos en caso de ser necesario y presentar dicho informe y sus evidencias cada vez que se realicen ajustes de sincronización.

- El protocolo de tiempo de red (NTP) se recomienda su uso en todos los dispositivos de red para mantener la hora sincronizada entre la infraestructura corporativa. También es recomendable activar mecanismos de seguridad para NTP para evitar ataques contra este protocolo

5.14. CONTROL DE SOFTWARE OPERACIONAL

Objetivo: Generar lineamientos y acciones que permitan asegurar la integridad y controlar la ejecución de software en los sistemas operativos.

Lineamientos:

- Se deben implementar mecanismo para controlar la instalación de software en sistemas operativos, este control podrá ser soportado con el proceso de gestión del cambio.

- Las siguientes directrices también deberán considerarse:

    - Actualización de software, aplicaciones y bibliotecas de sistemas de información las cuales solo debe ser ejecutada por los administradores con la debida autorización, manteniendo un registro o una bitácora de estas actualizaciones.

    - Los Sistemas en producción deben tener solamente código ejecutable aprobado. Código de desarrollo y compiladores pueden existir, debidamente restringidos y para uso solo en situaciones de excepción debidamente controladas.

    - Emplear estrategias de retorno (rollback) debe definirse antes que los cambios sean implementados.

- Versiones previas del software de aplicación se deben retener como una medida de contingencia.

5.14.1. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

Objetivo: Definir lineamientos y estrategias para evitar el aprovechamiento y exposición de vulnerabilidades técnicas en los sistemas de información e infraestructura tecnológica de IDEAM.

Lineamientos:

- La oficina de informática debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información y componentes de infraestructura tecnológica teniendo en cuenta lo siguiente:

  - Evaluar el nivel de exposición de la organización a estas vulnerabilidades
  - Documentar acciones preventivas, correctivas y riesgos asociados.
  - Establecer roles y responsabilidades para la gestión de vulnerabilidades.
  - Definir planes de acción para remediar vulnerabilidades.

5.14.2. RESTRICCIONES SOBRE LA INSTALACIÓN DE SOFTWARE.

Objetivo: Establecer e implementar controles para la restricción de instalación de software por parte de los usuarios.

Lineamientos:

- La entidad, deberá definir y documentar una línea base de las aplicaciones y software permitido dentro de la entidad, Para lo anterior los grupos de tecnologías y comunicaciones y de Sistemas de información deben tomar como base el catálogo de sistemas de información y software de infraestructura tecnológica para crear la línea base de dichas aplicaciones.

- La oficina de informática deberá realizar inspección a la infraestructura tecnológica y equipos de cómputo para verificar que estos sean de uso exclusivo para el desarrollo de funciones y/o obligaciones pactadas.

- La oficina de informática deberá realizar periódicamente la revisión y verificación del software instalado y ejecutado en los equipos de cómputo de IDEAM.

- Esta labor sólo puede ser realizada por la oficina de informática. Está prohibido que un usuario de la red o personal ajeno a la oficina de informática, realice actualizaciones de software o cambios en la configuración de hardware del equipo de cómputo.

- Se restringe el uso de aplicaciones y software no licenciado, en caso de requerir la ejecución y/o de algún software el cual es de libre distribución (no requiere licencia comercial), deberá solicitarse a la oficina de informática a través de la mesa de servicios, donde se emitirá un concepto técnico y respuesta a la solicitud.

- La oficina de informática autorizará y designará al personal para instalar, configurar y dar soporte tecnológico a los equipos de cómputo de IDEAM.

5.15. CONSIDERACIONES SOBRE AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

Objetivo: Definir lineamientos que permitan realizar el desarrollo de auditorías y verificación de los sistemas de información del IDEAM

Lineamientos:

- Se deberá coordinar un plan de auditoría considerando lo siguiente:

    - Definir alcances en el proceso de auditoría esto deberá acordarse con las diferentes partes interesadas.

    - Ejecución de pruebas de auditoría deberá realizarse en horario no laboral esto con el fin evitar afectaciones en la disponibilidad y prestación de servicios institucionales, esto será definido y coordinado con las partes interesadas.

- Documentar resultados del proceso de auditoría y acciones de mejora.

5.16. SEGURIDAD DE LAS COMUNICACIONES

5.16.1. GESTIÓN DE LA SEGURIDAD DE LAS REDES

Objetivo: Brindar lineamientos que permitan propender por la protección de la información en las redes de comunicación y sus instalaciones de procesamiento de información.

Lineamientos:

- La oficina de informática debe suministrar y poner en operación una plataforma tecnológica que cumpla con los requerimientos para soportar la operación de TI de todos los servicios institucionales implementados, este servicio de comunicaciones deberá contemplar lo siguiente:

  - Realizar una segmentación y separación de ambientes de redes, para servicios de TI y sistemas de información, para colaboradores y visitantes.

  - Se deberá mantener documentado las configuraciones del servicio de comunicaciones.

  - Restringir la comunicación de los puertos físicos y lógicos, esto con el fin de prevenir accesos no autorizados, la exposición de vulnerabilidades y posible generación de incidentes de seguridad, así mismo estos puertos deberán ser monitoreados.

  - El monitoreo de la infraestructura de red deberá ser revisado de forma regular para verificar que se conserven las configuraciones autorizadas y validar que no se evadan los controles y restricciones de red.

  - Implementar la segmentación (mínimo privilegio) en los recursos a los que se accederá de forma remota con el fin de garantizar que ante un acceso no autorizado al equipo que se está intentando

conectar a la red, no pueda acceder a recursos y/o información que no es necesaria para ese usuario

- Realice un monitoreo permanente a la infraestructura de los servicios utilizados, incluyendo a los teletrabajadores o trabajadores en casa, con el fin de analizar posibles acciones no autorizadas
- Controles de autenticación, cifrado y conexión de red.
- Activar perfiles de navegación para los usuarios SSL/VPN permitidos
- Parámetros técnicos necesarios para conexiones seguras.
- Procedimientos de restricción de acceso a los servicios y usos de red.

5.16.2. TRANSFERENCIA DE INFORMACIÓN

Objetivo: Definir lineamientos para preservar la seguridad de la información transferida entre la entidad y demás organizaciones.

Lineamientos:

- Establecer controles para el proceso de transferencia / intercambio de información con otras entidades públicas y/o privadas, a través de los servicios de comunicaciones de la Entidad.
- Emplear controles criptográficos y/o cifrados de datos para proteger la Integridad y confidencialidad de la información transmitida, no se permitirá el intercambio de información con otra entidad externa si este no dispone de un control de cifrado.
- Establecer controles para proteger la información transmitida a través del servicio de correo electrónico del IDEAM.

- Durante el proceso de transferencia se deberá tener presente la criticidad de la información transmitida, en caso de ser información crítica o que contenga datos personales sensibles deberán emplear controles de cifrado para la transferencia, esto con el fin de evitar la interceptación, copiado, alteración, modificación, sabotaje de la misma.

- Para la transferencia de información física propiedad del IDEAM, el grupo de Gestión documental, deberá definir los lineamientos para el proceso de transferencia, disposición y retención de la información física, acorde a la legislación y normativa legal vigente.

- Los servicios de navegación web serán otorgados únicamente para la misionalidad institucional y tendrán restricciones, en caso de requerir uso a servicios externos bien sea redes sociales, servicio de mensajería, entre otros, estos deberán ser solicitados de manera formal a la oficina de informática para la gestión respectiva.

5.17. ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN

Objetivo: Definir lineamientos para asegurar la confidencialidad y no divulgación de la información Institucional y requisitos necesarios para la protección de la información.

Lineamientos:

- Los acuerdos de confidencialidad o de no divulgación de la información deberán ser aplicables para los servidores públicos, Contratistas y partes externas de la entidad, teniendo en cuenta los términos legales y la normativa legal vigente.

5.18. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Objetivo: Definir lineamientos para que la gestión de la seguridad de la información sea parte integral de los sistemas de información de la Entidad.

5.18.1. ANÁLISIS Y ESPECIFICACIÓN DE REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Los requisitos referentes a la seguridad de la información, deberán contemplarse dentro de los requisitos para los nuevos sistemas de información o mejoras a los existentes.

Lineamientos:

- La Oficina de informática y el grupo de sistemas de información deberán documentar, controlar y formalizar la solicitud de requerimientos para nuevos sistemas de información, igualmente para las modificaciones que requieran ejecutarse para los sistemas de información existentes, teniendo en cuenta los siguientes aspectos de seguridad:
    - Gestión de acceso para los diferentes usuarios
    - Roles y responsabilidades
- La oficina de informática deberá establecer controles para el proceso de transferencia de datos a través de accesos públicos dispuestos para los sistemas de información de la entidad, manteniendo la privacidad y confidencialidad de la información de acuerdo con los niveles de clasificación.
    - Cifrado de comunicaciones
    - Aseguramiento en los protocolos de comunicación
    - Gestión de autenticación secreta de los usuarios
    - Acuerdos de confidencialidad entre las partes interesadas
- Emplear mecanismos que permitan la validación de usuarios a los sistemas de información "listas blancas".
- No exponer información personal o sujeta a reserva en enlaces de internet públicos cuyo acceso se genera sin autenticación. En caso que el enlace *(link)* sea generado por un código de respuesta rápida (QR), éste no debe tener identificadores que permitan fácilmente acceder a otros registros. Para tal fin se deben usar funciones de cálculo *hash* y otras formas de anonimización de datos.

5.18.2. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE.

Objetivo: Definir lineamientos para que la seguridad de la información sea diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.

Lineamientos:

- La entidad deberá mantener al menos 2 ambiente o entornos de trabajo: Pruebas y Producción:
    - Estos ambientes deben estar en diferentes segmentos de la red de comunicaciones de IDEAM.
    - Separación de bases de datos
    - Separación de roles en los distintos ambientes
    - No se permitirá realizar pruebas, instalación y/o desarrollos de software, sobre los entornos de producción
- Emplear tecnologías recientes para el desarrollo de sistemas de información
- Si la entidad debe habilitar un servicio en línea, primero deberá construir la matriz de riesgos (Formato habilitado por la oficina asesora de planeación) que permita identificar las brechas de seguridad que se generan a nivel de ciberseguridad, seguridad de la información e imagen institucional, antes de realizar la actividad, y procurando que las acciones de contingencia no afecten la seguridad de los datos
- Utilizar componentes que únicamente sean de orígenes oficiales de los fabricantes y que no impliquen riesgos para la entidad y la seguridad digital.
- La generación de código fuente deberá almacenarse controladamente en el repositorio designado para tener trazabilidad de las modificaciones y versionamiento en el proceso de desarrollo.
- Cuando se usen aplicaciones de mensajería instantánea estas deben garantizar el uso de encriptación extremo a extremo *(end-to-end)* y que tenga una política de privacidad y tratamiento de datos aceptable.

- El acceso a los códigos fuentes de los diferentes sistemas de información deberá ser restringido. Su acceso únicamente será gestionado por intermedio de las cuentas de acceso, privilegios asignados y autorización de acceso.

- Realizar copias de respaldo de los códigos fuentes cumpliendo con los requisitos de seguridad establecidos por el IDEAM.

- Los contratistas y/o proveedores y/o terceras partes, que tengan acceso y manipulen los códigos fuente de los sistemas de información críticos deberán suscribir un acuerdo de confidencialidad y no divulgación de la información.

- En caso de una interventoría o consultores externos los accesos solo serán otorgados en el periodo que requiera la ejecución de las actividades una vez culminado, los accesos deberán ser desactivados de forma inmediata.

- Realizar revisiones periódicas a los privilegios de usuarios en los sistemas de información y bases de datos, esto con el propósito de verificar y evitar la elevación de privilegios en las cuentas de usuario.

- Durante la configuración y aprovisionamiento de recursos y demás componentes que conforman los sistemas de información, evitar suministrar información, mensajes o características que permita a los atacantes recopilar información sobre las configuraciones y características del servicio.

- La oficina de informática a través de los grupos de sistemas de información y Tecnología y Comunicaciones y Líderes técnicos deberán coordinar y gestionar la revisión de todos los componentes de infraestructura, de esta manera asegurar que no se presenten vulnerabilidades que puedan comprometer los principios de seguridad de información.

    - Coordinar y realizar un análisis de posibles vulnerabilidades técnicas que puedan comprometer la operación de los sistemas de información, así la ejecución de actividades para la mitigación de estas.

- Los sistemas de autenticación de usuarios deberán emplear métodos de cifrado de información que no permita visualizar la información digitada, así mismo que no permita realizar la copia de credenciales de acceso en herramientas de texto plano o demás editores de texto.

- Los sistemas de información deberán emplear contraseñas que cumplan con los requisitos y características de generación de credenciales de acceso, todas las contraseñas de todos los usuarios que interactúan con los sistemas de información deben cumplir con estos requisitos, lo que incluye las cuentas de usuarios estándar, administradores y demás roles, además de esto deberá:

    - Evitar mantener configuraciones por defecto y el uso de las mismas.

    - Generar controles para las contraseñas débiles.

    - Controlar los inicios de sesión erróneos, definir medidas para la recuperación de acceso cuando se superan el límite de intentos fallidos y fortalecer los módulos de autenticación de usuario mediante un captcha para evitar ataques de fuerza bruta.

    - Controlar el ciclo de vida de las contraseñas en los sistemas de información.

    - Cerrar automáticamente y de forma controlada la sesión de un usuario cuando se detecte inactividad durante veinte (20) minutos.

    - Eliminar los identificadores de sesión una vez finalizada o cerrada la actividad en los sistemas de información.

- Deberá implementar controles de cifrado para la información sensible almacenada en los diferentes sistemas de información.

    - Evitar almacenar datos sensibles si no es estrictamente necesario.
    - Deshabilitar los almacenamientos en caché de la información sensible.

- Se debe establecer acuerdos y términos formales con entes externos, contratistas y/o proveedores, esto para asegurar la propiedad intelectual

cuando el proceso de desarrollo es tercerizado así mismo los niveles de confidencialidad de la información, tratada, procesada y/o generada en la ejecución de los nuevos proyectos.

- El ciclo de vida de los sistemas de información deberá hacer uso de procedimientos formales de control de cambios.

5.18.3. PROCEDIMIENTOS DE CONTROL DE CAMBIOS EN SISTEMAS DE INFORMACIÓN.

Objetivo: Controlar formalmente el ciclo de vida de desarrollo de sistemas de información mediante un proceso formal de control de cambios.

Lineamientos:

Los procedimientos formales de control de cambios se deberían documentar y hacer cumplir para asegurar la integridad del sistema, las aplicaciones y servicios de la entidad, del ciclo de vida de desarrollo.

La Gestión de cambios deberá considerar:

- Todo cambio deberá ser formalizado y solicitado a través de la mesa de servicios, posteriormente la aprobación por parte del comité de cambios y autorización para su ejecución.

- Mantener un registro de los niveles de autorización acordados

- Asegurar que los cambios son propuestos, presentados y aceptados por los usuarios autorizados.

- Identificar todo el software, la información, las entidades de bases de datos, hardware y componentes de TI que requieran modificaciones.
- Garantizar que la implementación se lleve a cabo minimizando potenciales riesgos o afectaciones a nivel de servicios.

- Asegurar que la documentación del sistema se actualiza cuando se completa el cambio y se archiva la documentación desactualizada.

- Mantener un control de versiones para todas las actualizaciones en los sistemas de información.

- Mantener registros de auditoría de todas las solicitudes de cambios.

- Asegurar que la documentación operativa y los procedimientos de usuarios se modifiquen según las necesidades.

- Asegurar que la persona que solicite el cambio y la que apruebe y haga los cambios no sea la misma (segregación de funciones).

- Informar a todas las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.

- Los sistemas de información previos a su despliegue en el ambiente productivo deberán incluir:

    - Pruebas de integración (instalación, almacenamiento, seguridad, configuración y recuperación ante errores)
    - Pruebas Funcionales
    - Pruebas no Funcionales
    - Pruebas de Desempeño, estrés y carga (rendimiento).

5.18.4. PROTECCIÓN DE DATOS DE PRUEBA

Objetivo: Asegurar la protección de los datos usados para pruebas.

Lineamientos:

- Los controles y restricciones de acceso definidos a los ambientes de producción también deben definirse y aplicarse a los ambientes de pruebas.

- La información operacional objeto de la realización de pruebas se debe eliminar del ambiente una vez finalizadas las pruebas.

- Los datos de prueba deberán ser seleccionados cuidadosamente, así mismo protegerse y controlarse teniendo en cuenta lo siguiente:

- No se permite la exposición de datos sensibles en los entornos de prueba.

- Se deberá restringir el uso de las bases de datos operativas en otros entornos.

- Los datos de prueba deben ser falsos, no extraídos de los datos reales. Si los datos son extraídos de los datos reales, se debe emplear el enmascaramiento de los datos, donde sea posible, para proteger la información clasificada y/o sensible de la entidad.

5.19. RELACIÓN CON PROVEEDORES

Objetivo: Asegurar la integridad, confidencialidad y disponibilidad de los activos de información de la entidad, que sean accesibles a contratistas y/o proveedores.

Lineamientos:

- La oficina jurídica, deberá establecer los lineamientos para el cumplimiento de obligaciones en lo referente a la seguridad y privacidad de la información del IDEAM así mismo deberá:

    - Suscribir acuerdos de confidencialidad y no divulgación de la información.
    - Autorización tratamiento de datos personales.
    - Derechos de propiedad intelectual y Derechos de autor.
    - En el caso de la oficina de informática y proveedores de servicios verificar mensualmente el cumplimiento de los acuerdos a nivel de servicios.

- La entidad debe establecer los criterios de selección y evaluación que incluyan aspectos como experiencia, reputación de los proveedores de servicios, así mismo certificaciones que acrediten la experiencia y la idoneidad para la prestación de servicios para IDEAM.

- La Oficina de informática debe establecer e implementar un procedimiento que permita asegurar la gestión de cambios a nivel de sistemas de

información, aplicaciones, y componentes de la plataforma tecnológica que son soportados y operados por terceras partes y/o proveedores.

- Cuando sea necesario, los aspectos de seguridad deben incluirse en el contrato. El detalle se definirá dependiendo del objeto contractual, servicio/sistema a ser tercerizado.

- La entidad debe asegurar la utilización de accesos y privilegios a los servicios de tecnología únicamente al personal autorizado, esta gestión deberá estar formalizada según como lo indica el procedimiento de gestión de accesos.

  - Los accesos otorgados deberán ser supervisados y controlados en el marco de la ejecución contractual y una vez finalizado estos accesos deberán ser retirados y/o modificados según el caso que aplique.

- En general, toda la información y los datos proporcionados por los funcionarios, contratistas, aspirantes/candidatos, proveedores y ciudadanos o que de otra forma sean recopilados en el contexto del IDEAM, serán utilizados por el IDEAM de conformidad con el Reglamento (UE) 2016/679 ("GDPR") y la Ley 1581 de 2012. Esto significa, en particular, que cualquier procesamiento de datos personales realizado por el IDEAM respetará los principios de legalidad, equidad, transparencia, limitación de propósito, limitación de almacenamiento, minimización de datos, precisión, integridad y confidencialidad.

5.20. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Gestionar oportunamente los incidentes de seguridad de la información, mediante un enfoque coherente y eficaz.

Lineamientos:

- La oficina de informática a través del grupo de arquitectura empresarial y seguridad de la información, deberá definir un procedimiento para la gestión de incidentes de seguridad de la información, así mismo la disposición de los medios y canales de comunicaciones para la atención de los mismos.

- Definir lineamientos para el cumplimiento frente a los tiempos de respuesta a incidentes.

- Para este fin se deberá registrar el reporte, gestión / atención y documentación respectiva y evidencia de los incidentes de seguridad.

- Llevar el asunto a una instancia superior (escalar) el incidente de seguridad en caso de requerirlo.

- El oficial de seguridad de la información del IDEAM deberá mantener el contacto apropiados con autoridades, grupos de interés en materia a la gestión de incidentes de seguridad de la información.

- La oficina de informática será la encargada de realizar la recolección de evidencias de los incidentes de seguridad de la información.

- Para la recolección de evidencias y el transporte de elementos, se debe realizar teniendo en cuenta el proceso de la cadena de custodia.

5.21. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

5.21.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: definir lineamientos que permitan preservar los principios de seguridad de la información, en la gestión de la continuidad del negocio, ante situaciones adversas, crisis o desastres.

Lineamientos:

- La oficina de informática, los grupos de trabajo y el oficial de seguridad de la información, deberán diseñar estrategias de recuperación de desastres que permitan suplir la operación crítica de TI de IDEAM, ante posibles incidentes y/o eventos que comprometan la disponibilidad de los mismos.

    - Dentro de las estrategias a desarrollar deberán incluir una gestión de incidentes y riesgos de Continuidad del negocio - servicios críticos institucionales.

    - Desarrollar un análisis de impacto de negocio BIA, para priorizar servicios e identificar servicios críticos.

- El plan de Recuperación de Desastres de IDEAM deberá incluir lo siguiente:

    - Roles y Responsabilidades.
    - Servicios Críticos.
    - Plan de pruebas basado en escenarios.
    - Informe de Resultados.
    - Árbol de comunicaciones.
    - Definir los RTO y RPO de la operación del servicio.
    - Sensibilización y/o entrenamiento.

        - Las pruebas de las estrategias de recuperación de desastres deberán estar integradas con el proceso de gestión del cambio,

- La ejecución de procesos a cargo de terceras partes deberá disponer de estrategias y planes de contingencia.

- Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques de seguridad de la información.

- Las estrategias de recuperación de desastres deberán ser revisadas según la necesidad de la entidad o en caso de surgir cambios en los diferentes contextos del IDEAM, además de esto deberá documentarse los planes de contingencia y recuperación de desastres.
    - Las estrategias de recuperación y planes de contingencia deberán ser revisados y aprobados por la alta dirección, así mismo deberá comunicarse al interior de la Entidad.

- Gestionar un manejo de crisis en caso de presentarse una eventualidad que comprometa la operación y servicios críticos.

5.21.2. DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN.

Objetivo: Las instalaciones de procesamiento crítico de información se deben implementar con redundancia necesaria para cumplir los requisitos de disponibilidad.

Lineamientos:

- La oficina de informática deberá identificar los requisitos para asegurar la disponibilidad de los sistemas de información y demás componentes de la plataforma tecnológica, con el objetivo de contemplar la implementación de componentes o arquitecturas redundantes.

- Los sistemas con redundancia deberán ser sometidos a prueba para verificar su respuesta ante posibles fallos.

5.22. CUMPLIMIENTO

Objetivo: Propender por el cumplimiento de las obligaciones legales, estatutarias, de reglamento y/o contractuales relacionadas con seguridad de la información y sus requisitos.

Lineamientos:

- Es deber de todos los funcionarios, contratistas y terceras partes de IDEAM, dar cumplimiento a las políticas de seguridad de la información, además de cumplir con los requisitos de la legislación y regulación institucional y del estado colombiano.

- La oficina de informática, a través del grupo de Arquitectura Empresarial y Seguridad de la Información y la oficina Asesora Jurídica deberá identificar, documentar y actualizar el normograma de todos los requisitos legales.

- La oficina de informática y la oficina asesora jurídica deberán definir controles con propósito de dar cumplimiento y protección de la propiedad intelectual, derechos de autos para los sistemas de información, licencias de software, códigos fuente.

    - Evitar copias o reproducciones y/o divulgaciones no autorizadas sin el consentimiento del propietario.

- La entidad deberá definir, aprobar y mantener actualizada una política para la regulación, tratamiento de datos personales conforme a la ley 1581 de 2012.

5.23. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN.

Objetivo: Asegurar que la seguridad de la información sea implementada y operable de acuerdo con las políticas y procedimientos del IDEAM.

Lineamientos:

- La oficina de informática y la oficina de control interno deberán coordinar para realizar de forma periódica/ regular procesos de auditorías internas para evaluar y verificar la implementación y operación del Sistema de Gestión de Seguridad de la Información en la Entidad.

- Los líderes de proceso, directores, subdirectores y jefes de oficina deberán propender por el cumplimiento de las políticas y procedimientos de seguridad de la información.

6. HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
1.0	01/12/ 2020	Primera versión Manual de políticas de seguridad de la Información.
2.0	18/05/2021	Segunda versión. Modificación de acuerdo a directiva presidencial 03 del 15 de marzo de 2021, recomendaciones consejería de transformación digital y recomendaciones de auditoria Externa

ELABORÒ:	REVISÒ:	APROBÒ:
		
Harbey Martínez Guerrero CISO IMPRECTICS - IDEAM	**Eduardo Ramírez Acosta** Coordinador GAESI Oficina de Informática	**Alicia Barón Leguizamón** Jefa Oficina de Informática