MANUAL DE IMPLEMENTACIÓN DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

Tabla de contenido

1 OBJETIVO

Orientar el accionar de los miembros de la comunidad universitaria explicitando aspectos técnicos que contribuyen a la adopción e implementación de lineamientos declarados en las políticas de seguridad y privacidad de la información.

2 ALCANCE

Los lineamientos y aspectos que se enuncian en el presente manual son aplicables a todos los procesos que gestionan información o activos de información institucional, se establecen en virtud de la adopción y cumplimiento de las políticas de seguridad y privacidad de la información.

3 DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001, capítulos A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4
- Modelo de Seguridad y Privacidad de Información (MSPI) – MinTIC.
- Manual Institucional de Políticas de seguridad y privacidad de la información.
- Inventario Institucional de activos de información.
- Manual de procedimientos administrativos para el tratamiento de datos personales, aprobado por la Resolución de Rectoría N.° 1227 de 2013.

4 DEFINICIONES Y ABREVIATURAS

- **ACTIVO DE INFORMACIÓN:** Equipo, persona, infraestructura, elemento o recurso utilizado para el tratamiento o almacenamiento de la información ya sea física o digital, considerada sensible o critica por la UAA para el desarrollo de sus funciones o prestación de sus servicios.
- **CIGyD:** Comité Institucional de Gestión y Desempeño**.**
- **CONTRATISTA**: Persona natural o jurídica, consorcio o unión temporal con quien se celebra el respectivo contrato. El contratista puede ser constructor, consultor, proveedor o prestador del servicio, entre otros, que se obliga a cumplir una determinada prestación, según las especificaciones del objeto del contrato, a cambio de una contraprestación.
- **CREDENCIALES DE ACCESO:** Par conformado por un nombre de usuario o "login" y una contraseña que identifica únicamente a cada uno de los usuarios y que les permite el acceso a los servicios de red o informático institucional.
- **DSI:** División de Servicios de Información.
- **DGTH:** División de Gestión del Talento Humano.

- **EGIS**: Equipo de Gestión de Incidentes de Seguridad.
- **EVENTO EN LA SEGURIDAD DE LA INFORMACIÓN:** Cualquier ocurrencia identificada en un sistema de información, servicio de tecnología o estado de la red, que implicó un cambio en sus operaciones diarias, indicando una posible infracción en la seguridad de la información, en la política o fallo en los controles, o una situación previamente desconocida que puede ser relevante para la seguridad. (Norma ISO 27002).
- **INCIDENTE EN LA SEGURIDAD DE LA INFORMACIÓN:** Cuando el evento se puede clasificar como no deseado o inesperado dentro de los eventos de seguridad de la información y además tienen una probabilidad significativa de comprometer las operaciones comerciales y suponen una seria amenaza para la seguridad de la información. (Norma ISO 27002).
- **LOGIN DE USUARIO:** Código de 8 letras formado con las iniciales o primeras letras de los nombres y apellidos del usuario miembro de la comunidad universitaria.
- **NIVEL DE ATENCIÓN**: Clasificación de la función o del rol en la recepción, detección y solución de un incidente de seguridad de la información.
- **RETIRO DE ACTIVOS DE INFORMACIÓN:** Extraer cualquier activo de información fuera de las instalaciones de la Universidad o del lugar habitual de trabajo.
- **ROL:** Perfil de un usuario de acuerdo a su tipo de vinculación institucional. Por ejemplo: docente, estudiante, empleado, personal invitado con autorización de alguna UAA.
- **SERVICIO DE RED O INFORMÁTICO:** Servicio de comunicación o de tratamiento de información ofrecido por la Universidad bajo la administración de una UAA. Por ejemplo: sistemas de información, Red WIFI, correo electrónico, servidores, bases de datos, entre otros.
- **SERVIDOR:** Un servidor es un equipo informático (físico o virtual) que forma parte de una red y provee servicios a otros equipos cliente.
- **UAA:** Unidad(es) Académico(s) Administrativa(s).
- **USUARIOS:** Miembro de la comunidad universitaria al cual se le autoriza acceso a algún servicio de red o informático según un Rol Institucional.
- **VPN:** Red privada virtual (Virtual Private Network).

5 NORMATIVA

- **Decreto 1360 de 1989** Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor.
- **Ley 527 de 1999** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 599 de 2000:** Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

- **Acuerdo 060 de 2001** Por el cual se establecen pautas para la administración de las comunicaciones oficiales en las entidades públicas y las privadas que cumplen funciones públicas.
- **Ley 1266 de 2008** Por la cual se dictan las disposiciones generales del *habeas data* y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1341 de 2009, Marco General del Sector de TIC** Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la información y las comunicaciones-TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- **Ley 1437 de 2011** Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Directiva Presidencial 04 de 2012** Eficiencia administrativa y lineamientos de la política cero papel en la administración pública.
- **Ley 1581 de 2012** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 1377 de 2013** Por la cual se reglamenta parcialmente la Ley 1581 de 2012 para la protección de datos personales.
- **Ley 1712 de 2014** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Decreto 1078 de 2015** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1080 de 2015** Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
- **Decreto 103 de 2015** Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Resolución 2710 de 2017** Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
- **Decreto 1008 de 2018** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
- **Resolución 1126 de 2021** Modifica plazo adopción IPv6, establecido en la Resolución 2710 de 2017.
- **Resolución 1674 de 2023** Por la cual se aprueba la Política de Privacidad y Seguridad de la Información de la Universidad Industrial de Santander.

6 ASPECTOS TÉCNICOS PARA GESTIONAR LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN INSTITUCIONAL

Los lineamientos y aspectos que se enuncian en el presente manual, se establecen en virtud de la adopción y cumplimiento de las políticas institucionales relacionadas con la seguridad y privacidad de la información. Con esto, se busca garantizar la integridad, disponibilidad y confidencialidad tanto de la información, como de los activos de información que se gestionan o producen desde los diversos procesos misionales y de apoyo de la Universidad. En consecuencia, cada UAA propenderá por ejecutar o implementar las acciones o proyectos pertinentes que permitan dar cumplimiento a los aspectos contenidos en el presente manual y políticas relacionadas con la información.

6.1 ASPECTOS RELACIONADOS CON LA POLÍTICA GESTIÓN DE PROYECTOS

Dentro de los elementos o instrumentos disponibles por la Universidad para reforzar los lineamientos relacionados con la política para gestión de los proyectos, en los casos que aplique, se pueden mencionar:

MECANISMO/INSTRUMENTO
Vicerrectoría de Investigación y Extensión - Políticas de derechos de autor - ACUERDO N.° 093 de 2010 - Procedimiento para la gestión de documentos contractuales con entidades aliadas o inicio de los proyectos de investigación con financiación interna - PIN.08 - Procedimiento para la gestión de documentos contractuales e inicio de proyectos de investigación con financiación externa - PIN.13

6.2 ASPECTOS RELACIONADOS CON LA POLÍTICA DISPOSITIVOS MÓVILES

Dentro de los elementos o instrumentos disponibles por la Universidad para reforzar los lineamientos relacionados con la política para gestión de los dispositivos móviles, en los casos que aplique, se pueden mencionar:

MECANISMO/INSTRUMENTO
Sección de Inventarios: - Manual normativo y procedimental para la administración y control de los bienes muebles de la UIS - MFI.02 División de Servicios de Información - Catálogo de Servicios (Instalación y Configuración de Software y Hardware) - Normas de uso de la red LAN

6.3 ASPECTOS RELACIONADOS CON LA GESTIÓN DEL PERSONAL

Los aspectos enunciados en este aparte están encaminados a la implementación de la "Política de seguridad de la información en relación a la gestión del personal" expuesta en el manual de políticas.

Consideraciones:

1. Estos aspectos aplican para todas las personas, naturales o jurídicas, que tienen un vínculo laboral, legal y reglamentario o contractual con la Universidad.
2. El proceso de vinculación de personal a la planta de la Universidad está a cargo de la DGTH.
3. La DGTH es la UAA encargada de brindar la concientización, sensibilización y capacitación del personal vinculado a la planta sobre los temas relacionados con la gestión de la seguridad y privacidad de la información.
4. Las actividades de sensibilización que tienen relación con contratistas o terceros, están a cargo de la UAA contratante.
5. Se deberán acatar los lineamientos o instrumentos definidos en la reglamentación institucional relacionados con la contratación, vinculación y formación de personal, tales como y entre otros:

MECANISMO/INSTRUMENTO
Dirección de Gestión de Talento Humano: - Procedimiento de entrenamiento y capacitación. - Plan institucional de entrenamiento y capacitación. - Acta de informe de gestión para entrega de cargos. - Código de Integridad de la Universidad Industrial de Santander. Resolución 0534 del 29 de abril de 2022. - Procedimientos de contratación según roles institucionales. Vicerrectoría de Investigación y Extensión: - Reglamento de Propiedad Intelectual. Acuerdo 093 de 2010 División de Contratación: - Estatuto y Reglamentación para la adquisición de bienes y servicios de la Universidad Industrial de Santander (Estatuto de Contratación) – Acuerdo C.S. n° 079 del 12 de diciembre de 2019. - Procedimientos de contratación según roles institucionales. Otras UAA: - Manual de funciones para los cargos de Empleados públicos no Profesionales y Trabajadores Oficiales de la Universidad Industrial de Santander. Acuerdo 104 de 2010. - Manual de procedimientos administrativos para el tratamiento de datos personales. Resolución 1227 de 2013 - Reglamento del Personal Administrativo. Acuerdo 074 de 1980 - Reglamento del Profesor. Acuerdo 063 de 1994

6. La Oficina de Control Interno Disciplinario es la dependencia encargada de adelantar las investigaciones disciplinarias a que haya lugar, en caso tal de presentarse alguna violación a las políticas de seguridad, en concordancia con la normativa vigente.
7. La Sección de Inventarios es la UAA encargada de brindar los lineamientos para la asignación y retiro de los activos de información a los funcionarios.
8. Temas sugeridos para sensibilización o capacitación, por ser considerados de alto riesgo por el personal:
    a. Gestión de credenciales de acceso.
    b. Uso de Inventarios.
    c. Presencia de Antivirus, Malware, correo no deseado.
    d. Software permitido y prohibido.
    e. Políticas de seguridad y privacidad de la información.
    f. Uso de correo electrónico institucional.
    g. Uso apropiado de Internet.
    h. Seguridad en los puestos de trabajo.
    i. Gestión de Incidentes de Seguridad.

6.3.1 VINCULACIÓN DE FUNCIONARIOS O CONTRATACIÓN DE EXTERNOS

La Universidad gestiona de manera segura la vinculación de funcionarios o contratación de externos en relación con la gestión de la seguridad y privacidad de la información, teniendo en cuenta:

1. Realizar las convocatorias de empleos o contratistas, de conformidad con la reglamentación institucional, para cada tipo de vinculación o contratación según los perfiles requeridos.
2. Realizar la investigación de antecedentes y referencias:
    a. Verificar las referencias pertinentes para la investigación de los antecedentes del postulante, determinando que sean satisfactorias, tales como:
        i. Certificaciones académicas.
        ii. Certificaciones laborales.
        iii. Referencias personales.
        iv. Confirmación de las calificaciones académicas y profesionales declaradas
        v. Identificación complementaria a la cedula de ciudadanía.
        vi. Antecedentes emitidos por los entes de control gubernamental: Procuraduría, Controlaría, Fiscalía, Policía, entre otros.
    b. Dependiendo del tipo de información y de los activos de información a los cuales tendrá acceso el aspirante, se podrá realizar una verificación más detallada de aspectos relativos a:
        i. Información crediticia.
        ii. Visitas domiciliarias.
        iii. Prueba de poligrafía.
        iv. Competencias necesarias para desempeñar el rol. etc.

3. Definir términos y condiciones o códigos de integridad o comportamiento del personal o contratistas, para el tratamiento de la información o de sus recursos o servicios de información, en los cuales se pueda apreciar, entre otros:
    a. Las responsabilidades sobre el manejo de la información institucional y conocimiento sobre las políticas de seguridad y privacidad de la información y uso de software licenciado.
    b. Los derechos sobre la propiedad intelectual y protección de datos.
    c. Las acciones a tomar en caso de omitir las políticas, procedimientos o requisitos de seguridad estipulados por la Universidad.
    d. Las responsabilidades relativas al manejo de la información recibida por otras entidades o entes externos.
    e. En caso de considerarse necesario, estipular las responsabilidades que continuarán vigentes a cargo del contratista o funcionario, durante un periodo de tiempo definido, posterior a la finalización del vínculo contractual, laboral o legal y reglamentario.
4. Asegurar la aceptación del tratamiento de la información de conformidad con lo establecido en las políticas de seguridad y privacidad de la información.
5. Organizar la documentación relacionada con el tratamiento de la información y datos personales, según las pautas archivísticas institucionales y lo establecido en las Tablas de Retención Documental.

6.3.2 CAPACITACIÓN Y SENSIBILIZACIÓN DE PERSONAL

La Universidad realiza la capacitación y sensibilización del personal y colaboradores, en temas de seguridad de la información teniendo en cuenta los diferentes roles y responsabilidades. Para ello, lleva a cabo acciones como:

1. Dar a conocer al personal (funcionarios, contratistas o terceros) las políticas, procedimientos, normas, leyes, reglamentos y códigos de ética relativos a la seguridad y privacidad de la información y protección de datos de personales, generando conciencia sobre:
    a. Amenazas y riesgos sobre el uso inadecuado de la información o de los activos de información.
    b. Canales dispuestos para reportar incidentes de seguridad detectados.
    c. Consecuencias derivadas del incumplimiento de las normas, políticas, reglamentos, entre otros, relativos a la seguridad de la información.
2. Velar por que el personal vinculado o contratado posea las competencias necesarias para desempeñar su rol de seguridad de la información:
    a. Garantizar que el personal a vincular posea los conocimientos básicos en el manejo de herramientas informáticas.
    b. Aplicar las políticas o procedimientos de seguridad de la información.
3. Indagar sobre las necesidades o falencias de los funcionarios y colaboradores en materia de seguridad de la información:
    a. Evaluar el resultado de aprendizaje de las sensibilizaciones o capacitaciones realizadas para identificar falencias.

   b. Aplicar encuestas que permitan identificar nuevos temas de sensibilización o capacitación.
   c. Reportar desde las UAA a la DGTH las necesidades de capacitación identificadas en los funcionarios adscritos a las mismas.
   d. Realizar el inventario sobre conocimiento de paquetes informáticos que permitan una gestión adecuada sobre la seguridad y privacidad de la información.
4. Proponer planes de capacitación o sensibilización pertinentes a la función, responsabilidades y habilidades del personal, en los cuales se incluyan, entre otras temáticas:
   a. El compromiso de la Dirección institucional con la seguridad y privacidad de la información.
   b. La importancia de divulgar y hacer cumplir la políticas, normas o leyes institucionales, locales o nacionales para el cumplimiento de las obligaciones en cuestión de seguridad y privacidad de la información.
   c. Las responsabilidades del personal en caso de infringir u omitir las normas de protección de la información.
   d. Los procedimientos básicos institucionales sobre seguridad de la información.
   e. Otros que considere importante la dirección de la Universidad.
5. Implementar estrategias de difusión que fomenten el conocimiento de las políticas de seguridad y privacidad de la información institucional.
6. Evaluar los espacios de formación llevados a cabo:
   a. Validar el cumplimiento de los objetivos.
   b. Identificar las debilidades y fortalezas, y la pertinencia de los temas expuestos.
   c. Destrucción del material que pueda contener información que comprometa información valiosa de la Universidad.

6.3.3 DESVINCULACIÓN DE PERSONAL

La Universidad gestiona de manera segura la desvinculación de funcionarios o contratistas en relación con la gestión de la seguridad y privacidad de la información, llevando a cabo acciones cómo:

1. Garantizar la devolución de los activos tangibles e intangibles de información a cargo, para ello el funcionario o contratista deberá:
   a. Realizar la entrega de los equipos o elementos que aparezcan a su cargo en el sistema de información de inventarios.
   b. Realizar la entrega de los elementos o equipos que se cedieron en condición de préstamos.
   c. Entregar la información generada en el desarrollo de sus actividades, así como los documentos institucionales que conoció en virtud de la realización de la actividad laboral o contractual.
   d. Retornar los dispositivos como: tarjetas de accesos, tarjetas de crédito, dispositivos móviles, medios de almacenamiento, entre otros, que la Universidad le haya asignado para el desarrollo de la actividad laboral o contractual.
2. Solicitar el retiro de los derechos de acceso a los activos de información, del personal desvinculado:

a. La UAA o la DGTH, según corresponda para contratistas o funcionarios respectivamente, solicitará a la DSI el retiro de los permisos de acceso asignados.
b. Las DSI desactivará o retirará los derechos de acceso asignados sobre los sistemas, servicios de información o listas de acceso a grupos institucionales, teniendo en cuenta el procedimiento definido para cada tipo de servicio de red o informático.

6.4 ASPECTOS RELACIONADOS CON LA GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Universidad realiza la gestión de sus activos de información por medio de los siguientes mecanismos institucionales:

MECANISMO/INSTRUMENTO
División de Servicios de Información: - Guía institucional para la identificación de activos de información. - Catálogo de servicios de la División de Servicios de Información. - Procedimiento para la prestación de servicios de tecnología de la información - PSI.10. - Procedimiento para la prestación de servicios de tecnología de la información en las sedes regionales - PSI.09. - Procedimiento para la gestión de credenciales de acceso a los sistemas de información institucionales – PSI.12 - Procedimiento para la gestión de credenciales de acceso al correo electrónico institucional – PSI.13 Sección de Inventarios: - Manual normativo y procedimental para la administración y control de bienes muebles - MFI.02. - Procedimiento para el ingreso de elementos al inventario – PFI.25 - Procedimiento para el seguimiento y control a los bienes muebles (Rendición de Inventarios y pruebas selectivas de inventarios) - PFI.20 - Procedimiento para el préstamo de bienes – PFI.21 - Procedimiento para dar de baja a elementos devolutivos e intangibles - PFI.26 - Procedimiento para donación de bienes muebles realizada por la universidad – PFI.22 - Procedimiento para el trámite de hurtos y pérdidas de elementos devolutivos – PFI.35 Dirección de Certificación y Gestión Documental: - Programa de gestión documental - PGGD.01 - Plan institucional de archivos – PINAR. - Instructivo para la organización de archivos de gestión - IGD.01 - Instructivo para las transferencias documentales - IGD.04 - Índice de información clasificada y reservada. - Instructivo para la eliminación documental - IGD.02 - Instructivo para la consulta de documentos de archivo - IGD.03 - Instructivo para las transferencias documentales - IGD.04

MECANISMO/INSTRUMENTO
- Instructivo para la organización de archivos de gestión en soporte digital e híbridos - IGD.07 - Instructivo para la digitalización de documentos - IGD.05 - Tablas de control de acceso. - Tablas de Retención Documental. - Sistema de Gestión de Documentos Electrónicos de Archivo SGDEA Dirección de Comunicaciones: - Manual de comunicación interna y externa - MCI.01. - Esquema de publicación de la información.

6.5 ASPECTOS RELACIONADOS CON EL CONTROL DEL ACCESO LÓGICO

A continuación, se enuncian los mecanismos que utiliza la Universidad para gestionar el acceso lógico a los servicios de red o informáticos que están bajo la custodia y administración de la DSI:

MECANISMO/INSTRUMENTO
División de Servicios de Información: - Catálogo de servicios de la División de Servicios de Información. - Normas de uso de la red LAN. - Normas de uso del correo electrónico institucional. - Procedimiento gestión de credenciales de acceso a los sistemas de información institucionales – PSI.12. - Procedimiento para la prestación de servicios de tecnología de la información - PSI.10 - Procedimiento para la prestación de servicios de tecnología de la información en Sedes Regionales - PSI.09. - Procedimiento para la gestión de credenciales de acceso al correo electrónico institucional – PSI.13. - Guía de Conexión Usuarios Wi-Fi Comunidad UIS. - Procedimiento para gestión de contraseñas de acceso a servicios informáticos - PSI.14 - Términos y condiciones de uso página web UIS – MSI.01 Dirección de Comunicaciones: - Tablas de control de acceso a documentos

6.6 ASPECTOS RELACIONADOS CON LA SEGURIDAD FÍSICA DEL ENTORNO SOBRE LOS ACTIVOS DE INFORMACIÓN QUE PROCESAN INFORMACIÓN SENSIBLE

6.6.1 CONTROLES DE ACCESO FÍSICO

Para gestionar el acceso físico de forma segura a las instalaciones críticas de procesamiento de información por parte del personal autorizado, en la Universidad, se tendrá en cuenta que:

1. La DSI define los roles de los funcionarios que pueden acceder a los centros de datos y centros de cableados.
2. Los funcionarios que ingresan a los centros de datos o centros de cableado, tienen definido el propósito de acceso y los elementos a los cuales pueden acceder de acuerdo a sus funciones.
3. El funcionario que haga uso de tarjeta o carnet de acceso a centros de procesamiento o almacenamiento de información institucional es responsable de su custodia, velando por su cuidado y protección, de manera tal que no sean extraviados, duplicados o alterados, o que sean utilizados para actividades fraudulentas.
4. El personal visitante, proveedores y contratistas prestadores de servicios:
    a. Requieren de una solicitud de acceso aprobada y controlada previamente por el responsable de la seguridad del área restringida.
    b. Portarán identificación en un lugar visible mientras permanezcan en los espacios autorizados.
    c. Estarán acompañados por un funcionario de la DSI, evitando realizar trabajos no supervisados y acciones maliciosas.
5. La DSI mantiene una bitácora de acceso de los usuarios, con fecha y hora de entrada y salida.
6. Las puertas de acceso están dotadas de sistemas de seguridad para controlar el acceso.
7. Los equipos de cómputo y servidores alojados en estos espacios, permanecen con credenciales de acceso que limitan su acceso lógico y físico.
8. Los derechos de acceso de los funcionarios, visitantes, proveedores o contratistas, serán actualizados regularmente y revocados cuando sea pertinente, en atención a la necesidad del servicio.
9. Para la desactivación del acceso de un usuario con permisos de acceso al Data CENTER o a los centros de cableado de la red de datos LAN institucional se requiere:
    a. Que la jefatura de la DSI notifique al funcionario administrador de la plataforma de control de los centros de cableado sobre la desvinculación del usuario.
    b. Que el funcionario administrador de la plataforma de control de los centros de cableado o del Data Center proceda a inhabilitar las credenciales de acceso del usuario reportado por la jefatura de la DSI.
10. A los usuarios que se encuentren en proceso de vacaciones o licencia no remunerada, les serán revocados los permisos de acceso y serán restablecidos una vez se incorporen a sus labores.
11. Los instrumentos establecidos para gestionar el acceso físico a las instalaciones de procesamiento de información, se establecen:

MECANISMO/INSTRUMENTO
División de Servicios de Información: - Procedimiento control de acceso físico a las instalaciones de procesamiento de información crítica. - Normativa de uso del CENTIC. División de Planta Física: - Manual de Seguridad y Vigilancia MRF.09

12. Para los activos de información de tipo documental en soporte físico o electrónico (series y subseries documentales), deberán tenerse en cuenta los lineamientos de la Dirección de Certificación y Gestión Documental respecto a requisitos técnicos para su consulta y acceso, entre ellos:

MECANISMO/INSTRUMENTO
Dirección de Certificación y Gestión Documental. - Índice de información Clasificada y Reservada. - Tablas de control de acceso a documentos

6.6.2 PROTECCIÓN FÍSICA DE LOS ACTIVOS DE INFORMACIÓN CRÍTICA

A continuación, se ilustran las acciones con las cuales la Universidad protege sus activos críticos de procesamiento de información, determinando su ubicación, aseguramiento, protección ante desastres naturales o amenazas físicas, entre otras.

1. Definir de manera clara la ubicación de las áreas o espacios que albergan elementos o recursos que almacenan o procesan información sensible y que son de acceso restringido.
2. Definir los perímetros de seguridad, dependiendo de los riesgos identificados y los requisitos de seguridad requeridos para la protección de los activos que forman parte del área restringida
3. Definir las características de los espacios que albergan los activos críticos, teniendo en cuenta:
    a. Adecuarlos para prevenir el acceso desde el exterior.
    b. Acondicionarlos con las barreras físicas y materiales adecuados, precaviendo posibles desastres naturales y previniendo simultáneamente la contaminación ambiental.
    c. Dotarlos de los mecanismos de respaldos requeridos; tales como, sensores de incendio, alarmas y cámaras de vigilancia, acondicionarlos con sistemas de protección a emanaciones electromagnéticas y monitorearlos para determinar su funcionalidad, en los casos que se considere necesario.
    d. Mantenerlos cerrados y sujetos a controles de acceso autorizado.

e. Proveerlos de un espacio de recepción con vigilancia a la entrada del edificio que permita supervisar el acceso físico.
f. Acondicionarlos de espacios físicos separados que permitan la administración y manipulación por personal externo a la DSI, como es el caso de data center.

4. Instalar las conexiones eléctricas y de comunicaciones de forma separada para reducir posibles interferencias.
5. Restringir la realización de algunas actividades en espacios o áreas con activos críticos, tales como: fumar, introducir alimentos o bebidas, uso de armas corto punzantes, trasladar, desconectar o conectar equipos o elementos sin autorización, modificar la configuración de los elementos o equipos sin autorización, instalar, desinstalar o alterar el software sin la autorización, alterar o modificar las etiquetas de las conexiones o equipos, extraer información de los equipos en dispositivos externos, acceder a elementos para los cuales no fue autorizado, realizar trabajos no supervisados, entre otras.
6. Almacenar y controlar según los lineamientos técnicos de la Dirección de Certificación y Gestión Documental el acceso a los activos de información de tipo documental en soporte físico (series y subseries documentales).
7. Dentro los instrumentos o mecanismos establecidos se pueden mencionar:

MECANISMO/INSTRUMENTO
Dirección de Certificación y Gestión Documental. - Tablas de Retención Documental

6.6.3 RETIRO Y BAJA DE LOS ACTIVOS DE INFORMACIÓN

A continuación, se explica cómo los activos de información deben ser retirados de la Universidad, indicando el nivel de autorización, flujo de solicitud y controles de seguridad a aplicar cuando se encuentren fuera de la Universidad:

1. Todo elemento que forme parte del inventario de activos de información y que requiera ser retirado, trasladado o dado de baja, contará con la aprobación del funcionario o instancia responsable, de conformidad con la reglamentación institucional tales como:
2. Entre los instrumentos para la gestión de baja y retiro de los activos de información se pueden mencionar, entre otros:

MECANISMO/INSTRUMENTO
Sección de Inventarios - Procedimiento Baja de Elementos Devolutivos e Intangibles – PFI.26. - Procedimiento Préstamo de Bienes – PFI.21 - Procedimiento Donación de Bienes Muebles Realizada por la Universidad – PFI.22 - Manual Normativo y Procedimental para la Administración y Control de los Bienes Muebles - MFI.02

División de Panta Física: - Manual de seguridad y vigilancia - MRF.09

3. Los equipos que se pretendan reutilizar, donar o dar de baja, y que contengan soportes de almacenamiento, serán borrados o desechados, utilizando técnicas de borrado seguro, de manera tal que no puedan recuperarse datos sensibles y software licenciado.
4. Los medios de almacenamiento que han sufrido daños y que además han almacenado datos sensibles, se destruirán físicamente en lugar de repararse.
5. Los tramites de retiro, baja o traslado de cualquier activo deberán ser registrados en el sistema de información, controlando la movilidad y custodia de dichos elementos hasta su baja o reingreso a la institución.
6. El retiro de un activo de información, fuera de las instalaciones de la Universidad, se realizará siguiendo el procedimiento definido para el manejo de bienes muebles institucionales y una vez autorizado el retiro se requiere:

   Por parte del responsable:

   i. No dejarlos desatendidos en lugares públicos para evitar daños o robos.
   ii. Manipularlos teniendo en cuenta los lineamientos dados por el fabricante.

   Por parte de la DSI o UAA propietaria del activo:

   iii. Mantener una bitácora con el nombre del personal externo o entidad que custodiará el activo y las actividades a realizar en él.
7. Para la eliminación de activos de información de tipo documental (series y subseries documentales), física o electrónica, deberán tenerse en cuenta los lineamientos e instrumentos establecidos por la Dirección de Certificación y Gestión Documental, tales como:

MECANISMO/INSTRUMENTO
Dirección de Certificación y Gestión Documental - Tablas de Retención Documental TRD - Tablas de Valoración Documental TVD.

6.6.4 MANTENIMIENTO DE ACTIVOS DE INFORMACIÓN CRÍTICO

Los aspectos enunciados a continuación definen cómo la Universidad lleva a cabo los mantenimientos preventivos o correctivos a los equipos considerados críticos, indicando la periodicidad, personal autorizado, recomendaciones de los proveedores y registros pertinentes:

1. Los mantenimientos son ejecutados aplicando los instrumentos de reglamentación institucional. Para tal fin, se pueden mencionar entre otros:

MECANISMO/INSTRUMENTO
División de Servicios de Información - Procedimiento de mantenimiento preventivo PRT.02. - Procedimiento de mantenimiento correctivo PRT.01.

2. Los activos de información se instalan y adecuan teniendo en cuenta las indicaciones y recomendaciones del fabricante.
3. Los mantenimientos son realizados por funcionarios y técnicos autorizados o, en su defecto, por personal externo. En cuanto al personal externo, previamente se valida su idoneidad y la de la empresa a la que pertenecen, cuando aplique.
4. Las ventanas de mantenimiento son programadas e informadas con anticipación a la comunidad universitaria que pueda verse afectada con el desarrollo de la actividad.
5. En caso de existir información sensible en los equipos que requieran mantenimiento, la DSI determinará el tipo de borrado que amerite.
6. Se realiza registro de los fallos encontrados o sospechosos y las fechas de los mantenimientos preventivos o correctivos aplicados a los equipos.
7. Una vez finalizado el mantenimiento se realizarán pruebas que garanticen el funcionamiento correcto del mismo.
8. A los activos que cuenten con pólizas de seguro, se les aplicarán los mantenimientos de conformidad con los términos y condiciones estipulados en los contratos de seguros suscritos con las compañías aseguradoras.
9. Para los activos de información de tipo documental, en soporte físico o electrónico (series y subseries documentales), deberán tenerse en cuenta los lineamientos de la Dirección de Certificación y Gestión Documental respecto a la conservación y preservación documental.

MECANISMO/INSTRUMENTO
Dirección de Certificación y Gestión Documental - Plan de conservación de documentos - SIC

6.7 ASPECTOS RELACIONADOS CON LA SEGURIDAD DE LAS OPERACIONES SOBRE LOS ACTIVOS DE INFORMACIÓN QUE PROCESAN INFORMACIÓN SENSIBLE

6.7.1 GESTIÓN DE CAMBIOS

A continuación, se ilustra cómo la Universidad realiza el control de cambios de forma segura, en los activos de información considerados críticos, servicios Informáticos e Infraestructura de Red, bajo la administración y custodia de la DSI:

1. En los casos que aplique, la solicitud de cambios en los activos en mención se realiza de conformidad con la reglamentación institucional, tales como:

MECANISMO/INSTRUMENTO
Dirección Institucional - Procedimiento gestión del cambio PDI.01 División de Servicios de Información: - Procedimiento para el soporte y mantenimiento de software – PSI.06.

2. Los cambios sobre los activos de información críticos son solicitados al jefe de la DSI, por el responsable del activo o por el jefe de la UAA, según sea el caso, para su aprobación. En la solicitud se requiere describir los detalles de los cambios a aplicar, definir un plan de trabajo que contemple la implementación de estos y los resultados esperados.
3. Antes de iniciar la implementación del plan de trabajo, se revisará:
    a. Que los controles y procedimientos de integridad o políticas de seguridad implementadas no se vean comprometidos por los cambios.
    b. La correlación con otros activos de información (sistemas de información, bases de datos, dispositivos de red, u otros).
4. La DSI mantendrá una bitácora de las solicitudes, de su nivel de aprobación y de la documentación pertinente sobre los cambios aplicados.
5. Si los cambios a aplicar requieren de un tiempo de no disponibilidad del servicio, se notificará con anticipación a las áreas afectadas sobre el tiempo requerido, en el que no se prestará el servicio.
6. Finalizada la implementación de los cambios, el solicitante validará los resultados de las pruebas de funcionamiento y la efectividad de los cambios de acuerdo con los requerimientos.
7. En caso de ser una implementación sobre los Sistemas de Información, el profesional a cargo del desarrollo solicitará el paso de los cambios al ambiente de producción de acuerdo con el procedimiento definido, manteniendo paralelamente un control de versiones sobre las actualizaciones del software.
8. El responsable de implementar los cambios reportará los mismos a los usuarios interesados.
9. Al implementar los cambios se preverá un plan de retorno, en caso de ser necesario regresar al estado anterior a los cambios.

6.7.2 GESTIÓN DE LA CAPACIDAD

A continuación, se enuncian las acciones que adelanta la Universidad para gestionar los recursos informáticos en los cuales se almacenan los sistemas de información, bases datos u otros elementos relacionados con los desarrollos y cómo son monitoreados de forma regular, permitiendo gestionar su capacidad de almacenamiento y rendimiento:

1. Ejecutar procesos en lotes, en determinadas franjas de tiempo de baja concurrencia, que permitan monitorear el funcionamiento de los servidores y de los procesos que se ejecutan en ellos.
2. Eliminar los archivos de reportes generados por sistemas de información, cuando estos superan un periodo de dos meses de creación.
3. Revisar de forma manual los archivos que ocupan un espacio considerable de almacenamiento y eliminarlo si se consideran innecesarios.
4. Evaluar la viabilidad de cierre definitivo de aplicaciones y determinar los momentos en que serán dadas de baja, en casos como: no uso, reemplazo por nuevas versiones, obsolescencia, cambios considerables en la infraestructura tecnológica, incompatibilidad, entre otras.
5. Revisar las consultas a las bases de datos cuando se detectan tiempos lentos de respuestas en los sistemas de información, con el fin de determinar aspectos que interfieran en su buen desempeño, tales como: cruces excesivos en tablas, la necesidad de separación de consultas, creación de tablas temporales o índices, entre otros.
6. Asignar mayor ancho de banda a aquellas aplicaciones o servicios que lo ameriten.
7. Determinar la necesidad de implementar procesos de virtualización en algunos servidores y servicios, según se requiera.

6.7.3 GESTIÓN DE LOS AMBIENTES DE OPERACIONES

La Universidad, por medio de la DSI, realiza la separación, transición y establecimiento de requerimientos entre los diferentes ambientes operacionales (desarrollo, prueba, producción), con el fin de evitar problemas operacionales que puedan ocasionar incidentes críticos, en pro de ello:

1. La DSI define la metodología para la gestión de los ambientes de programación, de los datos, sistemas operativos, servidores y sistemas de información institucional.
2. Dependiendo del estado en el cual se encuentran los desarrollos, dispone de tres o dos ambientes de trabajo, así: los nuevos desarrollos cuentan con los ambientes de desarrollo, pruebas y producción; y los desarrollos antiguos cuentan con los ambientes de preproducción (prueba) y producción.
3. Establece restricciones y controles de acceso a los datos, de forma separada para cada ambiente, según el rol de acceso requerido.
4. Establece que en ningún momento se realiza transferencia de datos desde el ambiente de pruebas al ambiente de producción y que los datos en los ambientes de pruebas difieren de los datos del ambiente de producción, salvo en aquellas particularidades de procesos que impliquen proyección de determinadas operaciones.
5. Documenta y define la metodología y lineamientos de programación, al igual que los requerimientos para la transferencia de los datos (bases de datos, código, librerías u otros) a los ambientes. Entre dichos lineamientos se pueden mencionar:

a. Solicitar la creación de los usuarios genéricos requeridos para establecer la conexión con el ambiente de trabajo de interés.
b. Solicitar la creación de la base de datos, suministrando el script respectivo para su creación e indicar el dimensionamiento de las tablas a 2 años o al que haya lugar.
c. Aplicar el proceso de estandarización y obtener firma de aprobación sobre el informe de revisión técnica.
d. Alojar en el servidor de versiones el software requerido para despliegue, junto con los demás archivos a que haya lugar: .ear, servicios, data source, librerías, login-config, entre otros.
e. Acatar el procedimiento definido para los casos de elaboración o mantenimiento de software y el procesamiento de datos.

6.7.4 GESTIÓN DEL CÓDIGO MALICIOSO

Para encarar las acciones contra código malicioso, la Universidad realiza el monitoreo y protección de la infraestructura tecnológica y servicios informáticos, estableciendo aspectos cómo:

1. Instalar y activar el antivirus institucional en las estaciones de trabajos y equipos servidores de propiedad de la Universidad, lo cual se realiza con apoyo de personal autorizado de la DSI, teniendo en cuenta la política de uso de software y licencias.
2. Mantener activada de forma permanente la opción de actualización automática de los sistemas operativos, opción habilitada en el momento de entrega del PC, acción que será responsabilidad de los usuarios de los equipos de cómputo.
3. Diseñar y ejecutar planes por parte de los administradores de los equipos y servidores que garanticen las actualizaciones del software para mitigar o corregir vulnerabilidades del sistema operativo.
4. Implementar firewall sobre la red de datos del campus universitario.
5. Implementar y administrar herramientas que permiten realizar:
    a. Monitoreo de la red: tráfico de red en tiempo real, puertos, equipos activos de red, etc.
    b. Monitoreo de la plataforma antivirus para equipos finales.
    c. Atención del NOC en horario laboral.
    d. Alarmas críticas las 24 horas.
    e. Correlación y análisis de log del NGfirewalll para los diferentes puntos de control (firewall perimetral, firewall Wlan, Firewall Servidores, Firewall Cableada).
    f. Filtrado de tráfico a través de ACL para protección de servicios críticos misionales.
6. Aplicar restricciones de descargas o de acceso a determinados sitios web que el fabricante de la infraestructura de seguridad identifique como contenido malicioso.
7. Ejecutar el procedimiento de incidentes de seguridad, una vez verificada la presencia de código malicioso.

8. Todo equipo o segmento de red conectado directamente a la LAN deberá acatar los lineamientos definidos en la política de código malicioso.

6.7.5 GESTIÓN DE COPIAS DE SEGURIDAD

Las copias de respaldo sobre la información que gestiona cada funcionario en virtud de las actividades a su cargo son de responsabilidad individual; es decir, que cada funcionario velará por la realización de las mismas teniendo en cuenta los lineamientos que al respecto se exponen en las políticas de seguridad y privacidad de la información.

Para el caso de los activos de información, que se encuentra bajo la custodia y administración de la DSI, las copias de seguridad se realizarán teniendo en cuenta el instrumento a continuación:

MECANISMO/INSTRUMENTO
División de Servicios de Información: - Guía para la realización de backup - GSI.02.

6.8 ASPECTOS RELACIONADOS CON LA SEGURIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES

6.8.1 ASEGURAMIENTO DE SERVICIOS EN LA RED

La Universidad protege la información que viaja por los servicios de red institucional por medio de la DSI, que aplica controles de seguridad para el acceso a la red cableada e inalámbrica, realizando monitoreo y seguimiento a acciones consideradas sospechosas, complementando dicho accionar con aspectos como:

1. Separar las responsabilidades del personal que gestiona la infraestructura de las redes de comunicación de la infraestructura de los sistemas de información.
2. Realizar la conexión a los servicios misionales a través de protocolos seguros, como SSH, SFTP, VPN, HTTPS.
3. Gestionar las conexiones de acceso remoto a través de VPN o HTTPS con credenciales de acceso y roles particulares de cada usuario.
4. Mantener registros de trazabilidad de:
    a. Las transacciones de creación, eliminación y modificación en datos considerados sensibles desde los sistemas de información.

   b. Los eventos de seguridad sobre los accesos desde y hacia a internet.
   c. Del acceso a la WIFI permitiendo la realización de auditorías sobre los eventos de seguridad ocasionados por dichos accesos.
5. Realizar periódicamente actividades de monitoreo, con el fin de identificar actividades atípicas en comparación con la línea base de funcionamiento de la red y de los dispositivos conectados.
6. Detectar actividades atípicas en algún servidor conectado a la red o dispositivo de red y proceder a ejecutar el procedimiento de gestión de incidentes.
7. Mantener activos solo los puertos LAN considerados necesarios para la conectividad de PC institucionales.
8. Segregar a nivel de capas de arquitecturas de red y VLAN los servicios de red, según los roles de usuarios de acceso definidos institucionalmente.

6.8.2 TRANSFERENCIA DE INFORMACIÓN ELECTRÓNICA

Los funcionarios o colaboradores de las UAA, cuando requieran transferir información entre sí o con entidades/usuarios externos, tendrán en cuenta, complementariamente a lo expuesto en las políticas, aspectos como:

1. La transferencia de información se deberá realizar a través de los medios de comunicación electrónicos institucionales habilitados para tal fin.
2. La transferencia de documentación e información electrónica se realizará de conformidad con los lineamientos establecidos por la Dirección de Certificación y Gestión Documental, según lo establecido en los instrumentos a continuación:

MECANISMO/INSTRUMENTO
Dirección de Certificación y Gestión Documental - Tablas de Retención Documental TRD - Tablas de Valoración Documental TVD.

3. Los canales de comunicación a utilizar para cada tipo de información y las posibles restricciones sobre los permisos para el uso de estos se determinan por la DSI y la Dirección de Comunicaciones, en concordancia con las políticas de seguridad y privacidad de la información y demás lineamientos institucionales
4. El uso y necesidad de firmas digitales, electrónicas o mecánicas en la transferencia de documentos, transacciones o mensajes de datos estarán sujetos a las directrices que emita la dirección de la Universidad, en concordancia con la legislación y reglamentación vigente, aplicable en la materia.
5. Se validará que la información a transmitir esté libre de contenidos maliciosos, mediante su depuración por medio del programa antivirus institucional.

6. Al transferir archivos ejecutables, comprimidos, cifrados u otro, se deberá contemplar que éstos pueden ser eliminados, inactivados o puestos en cuarentena de acuerdo a la configuración de seguridad del receptor.
7. La información a compartir o transmitir se realizará teniendo en cuenta el índice de información clasificada y reservada, etiquetando consecuentemente dicha información, según la restricción de accesibilidad y según el medio de comunicación utilizado. En caso de requerir asesoría para este caso, se podrá acudir a la Dirección de Certificación y Gestión Documental.
8. Se aplicarán controles preventivos que permitan proteger la información o los medios de comunicación en caso detectar comportamientos anómalos.
9. Antes de intercambiar información o software con cualquier entidad externa (ej.: proveedores de servicios, empresas de mantenimiento de software y hardware, empresas que manejan transacciones o procesamiento de datos, clientes, etc.), deberá suscribirse un contrato en el que se estipulen las características técnicas relativas a la transferencia de la información de forma segura, siendo esto responsabilidad de la UAA contratante.
10. Los acuerdos con terceros deben ser confeccionados de acuerdo con la Política de seguridad para proveedores.

6.8.3 TRANSFERENCIA INFORMACIÓN DOCUMENTAL

La transferencia de la documentación física se hará teniendo en cuenta los lineamientos definidos por la Dirección de Certificación y Gestión Documental, en instrumentos como:

-

MECANISMO/INSTRUMENTO
Dirección de Certificación y Gestión Documental - Tablas de Retención Documental TRD. - Tablas de Valoración Documental TVD. - Instructivo para las transferencias documentales – IGD.04.

6.9 ASPECTOS RELACIONADOS CON LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Universidad Industrial de Santander para gestionar los incidentes relacionados con la información digital dispone del EGIS (Equipo Gestión de Incidentes de Seguridad), atendiendo casos relacionados con LAN, WAN, VPN, correo electrónico, Sistemas de Información, WIFI, Data Center, Servidores y Bases de datos, y para ello, hace uso de la Guía de Gestión de Incidentes de Seguridad Digital, direccionando su accionar en cuatro (4) etapas:

a. Preparación

b. Detección y Análisis
c. Contención, Erradicación y Recuperación
d. Actividades Post-Incidentes.

Por su parte, el EGIS se activa en cuatro niveles de gestión y cada nivel debe realizar o apoyar las actividades de monitoreo, detección, diagnóstico y solución:

1. El primer nivel de atención corresponde a los administradores de servicios y usuarios de las UAA que detecten y diagnostiquen incidentes de seguridad.
2. El segundo nivel de atención corresponde a funcionarios al interior de la DSI con el rol de apoyo, y serán quienes aplicarán las acciones correctivas direccionadas por los líderes funcionales.
3. El tercer nivel de atención corresponde a funcionarios al interior de la DSI con el rol de líderes funcionales, los cuales son profesionales que tienen a cargo los activos de información o servicios misionales críticos (VPN, Correo Electrónico, Sistemas de Información, WIFI, Servidores y Bases de datos, Canales de Internet, Infraestructura de Red). A estos líderes se acudirá dependiendo del activo o servicio afectado.
4. El cuarto nivel de atención corresponde al líder de seguridad digital de la DSI quien realiza gestión de las herramientas globales de detección, diagnóstico y solución de incidentes.

A continuación, se ilustra el instrumento orientador para la gestión de incidentes de seguridad de la información:

MECANISMO/INSTRUMENTO
División de Servicios de Información - Guía para la gestión de incidentes de seguridad digital.

Para complementar la gestión del proceso de incidentes de seguridad de información, se resaltan aspectos como:

1. La Oficina de Control Interno Disciplinario será la dependencia encargada de adelantar las investigaciones a que haya lugar, en relación con los incidentes de seguridad y privacidad de la información, que involucren la violación o desconocimiento de la normativa institucional o nacional vigente por parte de algún servidor.
2. Los funcionarios, trabajadores y contratistas deberán comunicar/reportar eventos e incidentes relacionados con la seguridad y privacidad de la información, ante las instancias o autoridades institucionales y nacionales a que haya lugar.
3. Los funcionarios relacionados con el tratamiento de los incidentes de seguridad de la información deberán recibir formación con relación a la gestión de incidentes de esta índole.

6.10 ASPECTOS RELACIONADOS CON LA SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES O TERCEROS

La UAA que requiera permitir acceso a la información o a algún activo de información clasificado como sensible o crítico a proveedores o terceros, para poder adquirir un servicio o producto, tendrá en cuenta los siguientes aspectos técnicos y administrativos. Lo anterior, para dar cumplimiento a los lineamientos contenidos en la política de seguridad de la información:

En la etapa precontractual:

1. Definir el tipo de servicio o producto que debe suministrar un proveedor o tercero sobre el activo de información de interés. Por ejemplo: servicio de TI, servicio de logística, servicios financieros, componente de la infraestructura de TI.
2. Identificar e implementar los controles de seguridad de información requeridos para mitigar el impacto del acceso del proveedor o tercero, de conformidad con las Políticas de Seguridad de la Información definidas por la UIS.

Etapa contractual:

3. Suscribir el respectivo contrato con el proveedor, que perfeccione la relación comercial o la prestación del servicio a proveer, en el cual deberán incluirse las condiciones de manejo de la información o activos involucrados, según lo establecido en el estatuto de contratación de la Universidad, actividad previa a la entrega o acceso a la información.

   El contrato a suscribir deberá contemplar, entre otros, aspectos tales como:
   a. Términos y condiciones institucionales para el tratamiento aceptable e inaceptable de la información.
   b. Referenciar los requisitos legales y de regulación institucional sobre tratamiento y protección de datos personales.
   c. Derechos de propiedad intelectual, derechos de autor y establecer el mecanismo de cumplimiento de los mismos.
   d. La identificación de la información y el tipo de acceso a la información, a la que ambas partes tendrán acceso, al igual que el personal que accederá a ella.
   e. En caso de existir una cadena de suministro, esta deberá cumplir los términos y condiciones institucionales sobre el tratamiento de la información institucional.
   f. Acuerdos de confidencialidad, en los casos que se identifique la necesidad especial de confidencialidad.
4. Velar por el cumplimiento de los requisitos de seguridad establecidos con el proveedor.
5. Informar al proveedor los lineamientos para respuesta a incidentes de seguridad de información, establecidos por la Universidad.

6. Implementar junto con el proveedor o terceros controles que permitan mantener la integridad de la información o de los servicios involucrados en el tratamiento de la información, de conformidad con las Políticas de la Información e instrumentos archivísticos emitidos por la Universidad.
7. Definir e implementar controles para la identificación y acceso del personal que conocerá la información y accederá a las instalaciones de tratamiento de información, informando consecuentemente los retiros de información por parte del personal que se presenten.
8. Establecer espacios o jornadas que permitan la sensibilización y concienciación del personal contratista en el manejo adecuado de la información o de los activos de información.

Etapa post-contractual:

9. Solicitar la restricción de acceso a los activos de información a los cuales fueron autorizados durante el proceso de contractual.
10. Recopilar la información suministrada y generada durante el proceso contractual y preservarla de acuerdo a los lineamientos institucionales para la gestión documental.

6.11 ASPECTOS RELACIONADOS CON LA GESTIÓN DE LA CONTINUIDAD DE LAS FUNCIONES INSTITUCIONALES

La Universidad, por medio de las UAA, adopta e implementa requisitos de seguridad de la información relacionados con la continuidad de sus funciones. Lo anterior, incorporando acciones desde la planificación de sus procesos y funcionamiento de los activos de información de misión crítica, como es el caso de los centros de datos, redes de datos y sistemas de información. Los siguientes aspectos se establecen para hacer frente a situaciones adversas o disruptivas que atenten contra el funcionamiento de la Institución:

1. Definir los requisitos y controles de seguridad de la información que requieran los activos de información de misión crítica, con el fin de mantenerlos en funcionamiento.
2. Gestionar la estructura tecnológica pertinente y mantenerla preparada, al igual que el personal con la competencia y experiencia necesaria, para gestionar la situación adversa.
3. Definir las herramientas y controles pertinentes, que permitan garantizar las condiciones de funcionalidad de la estructura implementada, para afrontar las eventuales situaciones adversas.
4. Definir, documentar y socializar con el personal involucrado los planes de respuesta y recuperación, que detallan como la UAA gestionará y mantendrá la seguridad de la información ante una situación adversa, para los activos de misión crítica.
5. Establecer los procesos, acciones y tiempos en los cuales los proveedores o terceros deben actuar, cuando se presenten situaciones adversas.
6. A continuación, se ilustran los instrumentos que orientan la gestión de la continuidad de las operaciones en los activos de misión crítica:

MECANISMO/INSTRUMENTO
División de Servicios de Información - Guía para la gestionar la continuidad de las operaciones.

6.12 ASPECTOS RELACIONADOS CON EL CONTROL DE SOFTWARE

Los aspectos que se enuncian a continuación permiten garantizar el control, uso, mantenimiento e instalación de software autorizado y no autorizado al interior de la Universidad:

6.12.1 CONTROLAR EL SOFTWARE AUTORIZADO

1. La instalación de software en equipos de la Universidad solo podrá realizarse por parte del personal calificado y autorizado de la UAA o de la DSI, teniendo en cuenta la política de uso de software y licencia. En el caso de que la UAA no disponga del personal, podrá solicitar apoyo a la DSI.
2. Para la instalación de software en los equipos institucionales se dispone del Sistema de Gestión de Solicitudes y del Catálogo de servicios de la DSI.
3. Cuando se gestione la adquisición de software especializado la UAA contratante deberá adquirirlo con el servicio de instalación y puesta a punto.
4. La UAA que requiera el apoyo de la DSI para la instalación de software, deberá:
    a. Ingresar la solicitud por el medio dispuesto para tal fin.
    b. Suministrar la siguiente información:
        i. Descripción detallada del requerimiento.
        ii. Número del inventario del equipo.
        iii. La ubicación del equipo: sede, edificio, piso, oficina
        iv. El horario de disponibilidad para la atención del técnico de la DSI
        v. Persona de contacto en la UAA.
5. La UAA contratante del licenciamiento supervisará que:
    a. La instalación se haga solo en equipos de cómputo que formen parte del inventario institucional, validando que cuenten con la identificación utilizada por la Universidad.
    b. El número de licencias instaladas no supere el adquirido.
6. Al finalizar la instalación, tanto el funcionario de la UAA como el personal que haga la instalación, diligenciarán el formato que evidencie el soporte realizado.

6.12.2 CONTROLAR EL SOFTWARE NO AUTORIZADO

1. No está permitido el uso de software sin el licenciamiento autorizado, tal como lo indica la política de seguridad de la información de la Universidad.
2. La verificación del software instalado en los equipos de cómputo institucional lo podrá realizar la Dirección de Control interno y Evaluación de Gestión y las UAA con el apoyo de la DSI, en caso de ser requerido.

3. Los funcionarios que detecten software no licenciado en los equipos de cómputo informarán al jefe de la UAA y procederán a la desinstalación del mismo.
4. Las UAA realizarán verificación periódica, para garantizar que los equipos que usan sus funcionarios cumplan con la política de uso de software y licencias. En caso de detectar software que no cumpla con los licenciamientos respectivos, el funcionario adelantará las acciones pertinentes, de conformidad con los procedimientos institucionales.
5. La Dirección de Control Interno y Evaluación de Gestión podrá definir de forma aleatoria las UAA para hacer control y verificación de uso de software legal. En caso que se detecte incumplimiento a la política de uso de software, adelantará las acciones pertinentes de conformidad con los procedimientos institucionales.

6.12.3 DESARROLLO Y MANTENIMIENTO DE SOFTWARE

El software desarrollado al interior de la Universidad, por parte de la DSI, es gestionado acatando las directrices expuestas en los siguientes instrumentos:

MECANISMO/INSTRUMENTO
División de Servicios de Información - Procedimiento para el soporte y mantenimiento de software – PSI.06 - Procedimiento de desarrollo de software – PSI.11 - Catálogo de Servicios de la División de Servicios de Información.

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIOS REALIZADOS
01	Abril 15 de 2024	Creación del documento