Universidad Industrial de Santander

CONSTRUIMOS FUTURO

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROCESOS: GESTIÓN DOCUMENTAL Y SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES

BUCARAMANGA

NOVIEMBRE 2023

CONTENIDO

Pág.

1 INTRODUCCIÓN 7

2 OBJETIVO 7

3 ALCANCE 7

4 NORMATIVIDAD 7

5 DOCUMENTOS DE REFERENCIA 9

6 GLOSARIO DE TÉRMINOS Y DEFINICIONES 9

7 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 11

7.1 Objetivos 11

7.2 Lineamientos. 12

7.3 Roles y responsabilidades 13

7.4 Alcance/Aplicabilidad 16

7.5 Nivel de cumplimiento 16

7.6 Revisión de la política de seguridad de la información 16

7.7 Entrada en vigencia y modificación 17

8 POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. 17

8.1 ORGANIZACIÓN INTERNA 17

8.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN GESTIÓN DE PROYECTOS 17

8.1.2 POLÍTICA DE DISPOSITIVOS MÓVILES 18

8.1.3 POLÍTICA DE TRABAJO EN CASA PARA LA SEGURIDAD DE LA INFORMACIÓN 20

8.1.4 POLÍTICA PARA USO DE CONEXIONES REMOTAS 20

8.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN A LA GESTIÓN DEL PERSONAL. 21

8.2.1 Incorporación de la seguridad de la información en las responsabilidades de personas funcionarias y contratistas. 22
8.2.2 Acuerdo de Confidencialidad. 22
8.2.3 Selección y vinculación de personal a la planta. 22
8.2.4 Términos y Condiciones Laborales 24
8.2.5 Responsabilidades de las personas pertenecientes a la comunidad universitaria. 24
8.2.6 Responsabilidades del estudiantado. 25
8.2.7 Responsabilidades de Usuarios Externos 25
8.2.8 Entrenamiento, concientización y capacitación 25
8.2.9 Desvinculación, licencias, vacaciones o cambio de labores de personas funcionarias y personal provisto por terceros. 26
8.2.10 Procesos disciplinarios. 27
8.3 GESTIÓN DE ACTIVOS DE INFORMACIÓN DE SEGURIDAD DIGITAL 27
8.3.1 Generalidades 27
8.3.2 POLÍTICA PARA LA GESTIÓN DE CENTROS DE PROCESAMIENTO Y DE CABLEADO. 29
8.3.3 POLÍTICA USO DE LOS SISTEMAS DE INFORMACIÓN 30
8.3.4 POLÍTICA USO DE SOFTWARE Y LICENCIAS 30
8.3.5 POLÍTICA PROTECCIÓN Y USO DE LAS ESTACIONES CLIENTE DE TRABAJO 32
8.3.6 POLÍTICA PARA ADMINISTRACIÓN DE SERVIDORES Y BASES DE DATOS. 34
8.3.7 POLÍTICA DE SOPORTE Y MANTENIMIENTO DE RECURSOS Y SERVICIOS INFORMÁTICOS. 35
8.4 POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN 36
8.4.1 Generalidades 36
8.4.2 Esquema de Clasificación de la Información 37
8.4.3 Etiquetado y manejo de Información 37
8.4.4 Administración de los Archivos 38
8.5 GESTIÓN DE MEDIOS DE ALMACENAMIENTO 39

8.5.1 POLÍTICA PARA GESTIÓN Y DISPOSICIÓN DE MEDIOS REMOVIBLES 39
8.5.2 POLÍTICA DE BORRADO SEGURO 40
8.5.3 POLÍTICA PARA LA TRASFERENCIA DE MEDIOS FÍSICOS 41
8.5.4 POLÍTICA SOBRE ALMACENAMIENTO 41
8.5.5 POLÍTICA PARA EL PRÉSTAMO DE RECURSOS INFORMÁTICOS 42
8.5.6 POLÍTICA USO DE SISTEMAS DE VIDEOVIGILANCIAS 43
8.5.7 POLÍTICA SOBRE LOS SERVICIOS DE COLABORACIÓN 44
8.6 POLÍTICA DE USO DE CORREO ELECTRÓNICO 45
8.6.1 Generalidades 45
8.6.2 Límites en el número de mensajes enviados por correo 46
8.6.3 Cuentas de correo funcional institucional 46
8.6.4 Cuentas de correo personal institucional 47
8.6.5 Responsabilidades de los usuarios 48
8.6.6 Uso indebido del correo electrónico 49
8.6.7 Responsabilidades de la universidad 50
8.6.8 Manejo de casos excepcionales 50
8.6.9 Cuentas de correo en el dominio @uis.edu.co 51
8.6.10 Cuentas de correo en el dominio @correo.uis.edu.co 51
8.6.11 Listas de distribución de correo. 52
8.7 POLÍTICA DE ADMINISTRACIÓN DE LA RED INSTITUCIONAL 53
8.7.1 Uso aceptable del servicio 53
8.7.2 Responsabilidades de la División de Servicios de Información 55
8.7.3 Uso indebido de la Red LAN 55
8.8 POLÍTICA DE USO DE INTERNET. 56
8.8.1 Uso aceptable del servicio 57
8.8.2 Responsabilidades de los usuarios 58
8.8.3 Responsabilidades de la División de Servicios de Información 58
8.8.4 Uso Indebido de Internet 59

8.9 POLÍTICA DE REDES SOCIALES 60

8.9.1 Uso aceptable del servicio. 60

8.9.2 Uso indebido del servicio 61

8.10 POLÍTICA TRATAMIENTO DE DATOS PERSONALES 61

8.10.1 Anonimización de datos personales 62

8.11 CONTROLES DE ACCESO LÓGICO 63

8.11.1 POLÍTICA DE CONTROL DE ACCESO A REDES Y SERVICIOS EN RED 63

8.11.2 POLÍTICA ADMINISTRACIÓN DE LOS ACCESOS DE LOS USUARIOS 64

8.11.3 POLÍTICA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN UIS 70

8.12 POLÍTICA SEGURIDAD FÍSICA Y DEL ENTORNO 71

8.12.1 ÁREAS SEGURAS 72

8.12.2 SEGURIDAD DE LOS EQUIPOS 76

8.13 POLÍTICA SEGURIDAD DE LAS OPERACIONES 81

8.13.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES 81

8.13.2 SOFTWARE MALICIOSO 84

8.13.3 RESPALDO DE LA INFORMACIÓN 86

8.13.4 REGISTRO Y SUPERVISIÓN 87

8.13.5 CONTROL DE SOFTWARE EN PRODUCCIÓN 90

8.13.6 GESTIÓN DE VULNERABILIDAD TÉCNICA 91

8.13.7 CONSIDERACIONES SOBRE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN 93

8.14 SEGURIDAD DE LAS COMUNICACIONES 94

8.14.1 POLÍTICA GESTIÓN DE LA SEGURIDAD DE RED 94

8.14.2 POLÍTICA INTERCAMBIO DE INFORMACIÓN 96

8.15 POLÍTICA SOBRE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN 99

8.15.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN 99

8.15.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE 101

8.15.3 DATOS DE PRUEBA 106
8.16 POLÍTICA RELACIÓN CON PROVEEDORES 106
8.16.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES 107
8.16.2 GESTIÓN DE LA ENTREGA DEL SERVICIO POR PROVEEDORES 109
8.17 POLÍTICA GESTIÓN DE INCIDENTES Y MEJORAS DE SEGURIDAD DE LA INFORMACIÓN. 110
8.17.1 Responsabilidades y procedimientos 110
8.17.2 Reporte de eventos y vulnerabilidades de seguridad de la información 111
8.17.3 Evaluación y decisión sobre los eventos de seguridad de información. 112
8.17.4 Respuesta a incidentes de seguridad de la información 112
8.17.5 Gestión de conocimiento sobre los incidentes de seguridad de la información 112
8.17.6 Recolección de evidencia 112
8.18 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DE LAS FUNCIONES INSTITUCIONALES 113
8.18.1 Gestión de la continuidad de las funciones 113
8.18.2 ASPECTOS DE LA REDUNDANCIA EN RELACIÓN A LA CONTINUIDAD DE LAS FUNCIONES 114
8.18.3 RESPALDO DE INFORMACIÓN EN RELACIÓN A LA CONTINUIDAD DE LAS FUNCIONES 114
8.19 POLÍTICAS DE CUMPLIMIENTO LEGAL 115
8.19.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES 116
8.19.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN 118

1 INTRODUCCIÓN

Las entidades en su quehacer misional producen, recopilan y comparten una variedad de información que dependiendo de su importancia requiere de una gestión concienzuda que les permita garantizar los niveles de accesibilidad, de disponibilidad y de completa integridad. La Universidad Industrial de Santander es consciente de dicha necesidad y responsabilidad y, más aún, su carácter de entidad del Estado la hace heredera de adoptar mecanismos para direccionar su función pública. Dentro de esos mecanismos están los planes institucionales y estratégicos, entre los cuales se pueden mencionar el plan de seguridad y privacidad de la información; el plan de tratamiento de riesgos de seguridad y privacidad de la información y el plan estratégico de tecnologías de la información y las comunicaciones (PETI). Planes que, adicionalmente, están enmarcados dentro de la estrategia de Gobierno Digital, antes Gobierno en Línea.

La Universidad encamina acciones que le permiten realizar una mejor gestión de la información institucional generada desde sus diferentes procesos, en pro de velar por la seguridad de esta. En correspondencia con lo expuesto, con este documento se adoptan directrices y controles, condensados en políticas de seguridad y privacidad de la información, para unificar y direccionar el accionar de los miembros de la comunidad hacia una gestión eficiente y eficaz de la información y de los activos de información institucionales.

2 OBJETIVO

Establecer las normas y lineamientos para gestionar de manera adecuada la seguridad y privacidad de la información que recibe, maneja, transporta, genera o almacena la Universidad en función de sus actividades misionales.

3 ALCANCE

Lo dispuesto en este documento es aplicable a todos los procesos que gestionan información o activos de información institucional, siendo de obligatorio cumplimiento por parte de los miembros de la comunidad universitaria desde las diferentes unidades académico-administrativas.

4 NORMATIVIDAD

- Resolución 1126 de 2021. Modifica plazo adopción IPv6, establecido en la Resolución 2710 de 2017.
- **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 2710 de 2017. Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
- 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 103 de 2015.** Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **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 1377 de 2013** Por la cual se reglamenta parcialmente la Ley 1581 de 2012 para la protección de datos personales.
- **Ley 1581 de 2012** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 2609 de 2012** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Ley 1437 de 2011**: Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo y aplicación de criterios de seguridad.
- **Directiva Presidencial 04 de 2012** Eficiencia administrativa y lineamientos de la política cero papel en la administración pública.
- 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 1266 de 2008** Por la cual se dictan las disposiciones generales del hábeas 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.
- **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 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.

- **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.

5 DOCUMENTOS DE REFERENCIA

- Manual de gobierno digital: Implementación de la política de gobierno digital.
- Modelo de Seguridad y Privacidad de Información (MSPI) – MinTIC
- 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
- Guías del MinTIC, anexas para la implementación del Modelo de Seguridad
- Inventario de activos de información institucional
- Guía para la administración del riesgo y el diseño de controles en entidades públicas.
- Manual de procedimientos administrativos para el tratamiento de datos personales.

6 GLOSARIO DE TÉRMINOS Y DEFINICIONES

- **ACTIVO**: cualquier cosa que tenga valor para la organización[1]. Existen diversos tipos de activos en una organización como: información, software, programas de computador, físicos como los computadores, servicios, la gente y sus aptitudes, habilidades, y experiencia, intangibles como reputación o Imagen.
- **ACTIVO DE INFORMACIÓN**[2]: en relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN**[3]**:** Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales

[1] Norma ISO 27000
[2] MinTIC – Modelo de Seguridad y Privacidad de la Información
[3] Departamento Administrativo de la Función Pública - Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 octubre 2018.

como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.

- **ANONIMIZACIÓN:** La anonimización[4] es el proceso mediante el cual se condiciona un conjunto de datos de modo que no se pueda identificar a una persona, pero pueda ser utilizada para realizar análisis técnico y científico válido sobre ese conjunto de datos (MIT, 2007).
- **CONTINUIDAD DEL NEGOCIO:** Es la gestión de garantizar la continuidad de las operaciones y servicios críticos institucionales, ante situaciones adversas, que se están ejecutando o soportadas sobre la infraestructura de TI, apoyándose de manera simultánea en mecanismos de redundancia.
- **CORREO ELECTRÓNICO:** servicio que permite a los usuarios enviar y recibir mensajes electrónicos mediante la plataforma que la Universidad provee a la comunidad universitaria para facilitar la gestión y la comunicación.
- **CORREO SOSPECHOSO:** mensaje de correo cuyo remitente es desconocido, existen dudas sobre su existencia o inconsistencias respecto a su autoría.
- **CORREO NO DESEADO (CORREO SPAM):** mensaje de correo no solicitado, no esperado, o con remitente no conocido. Generalmente enviados masivamente y/o con contenido publicitario.
- **CUENTA DE CORREO PERSONAL INSTITUCIONAL:** aquella cuenta de correo en la que la dirección contiene el nombre y/o apellido del usuario, parte de ellos o una aproximación abreviada de ambos, con la extensión @uis.edu.co o @correo.uis.edu.co.
- **CUENTA DE CORREO FUNCIONAL INSTITUCIONAL:** aquella cuenta de correo en la que la dirección es genérica, es decir, no está asociada a una persona específica, sino a un propósito o función, UAA, evento, congreso, grupo o centro de investigación, entre otros, con la extensión @uis.edu.co.
- **DATOS SENSIBLES:** Datos que requieren ser protegidos con un uso adecuado evitando fuga de información que pueda producir sanción de índole financiero o disciplinario.
- **DSI**: División de Servicios de Información
- **INFORMACIÓN**[1]: Datos relacionados que tienen significado para la institución. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.
- **LISTA DE DISTRIBUCIÓN DE CORREO:** es una colección de cuentas de correo electrónico creada con un nombre de la forma nombre_lista@uis.edu.co a través de la cual se pueden enviar correos a todas las cuentas que la conforman.
- **LOG**: A nivel informático es considerado una especie de bitácora, en la cual se registran las acciones, a manera de evidencia, que permiten conocer la trazabilidad de las operaciones realizadas sobre determinado servicio o información sistematizada.

[4] Archivo General de la Nación Colombia - Guía de Anonimizarían de Datos Estructurados - https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/Guia_de_Anonimizacion-min.pd

- **POLÍTICA**: El artículo 6 del acuerdo 034 de 2019 del Consejo Superior de ña Universidad, estable que: "en el Modelo Integrado De Planeación Y Gestión - MIPG que se implemente, la expresión 'política' en relación con la gestión y desempeño institucional de la Universidad Industrial De Santander corresponderá a los lineamientos que contendrán planes, programas, proyectos, metodologías y estrategias descritas, existentes o implementadas en concordancia con la reglamentación aplicable"
- **REDUNDANCI**A: En informática es considerada la capacidad que se tiene para asegurar la funcionalidad de un activo (hardware o software) de carácter crítico ante posibles fallas, estableciendo un mecanismo de respaldo o de funcionamiento alterno permitiendo la continuidad del negocio o la alta disponibilidad del activo. Ejemplos: Servidores espejos, bases de datos simultaneas, suministro de corriente alterno.
- **REGISTRO**[5]: Es un documento que presenta los resultados obtenidos o proporciona evidencia de una actividad realizada. Ejemplo: la evaluación de proveedores es un registro, el despliegue de objetivos e indicadores es otro registro, la tecnomecánica de un vehículo es otro registro; cuando la sellan y firman dejan evidencias de que se ha pasado la inspección técnica del vehículo.
- **UAA**: Unidad(es) Académico Administrativa(s).
- **UIS**: Universidad Industrial de Santander.
- **USUARIO: miembro de la comunidad universitaria** que hace uso de los servicios de la red LAN institucional.

7 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La UNIVERSIDAD INDUSTRIAL DE SANTANDER, entendiendo la importancia de una adecuada gestión de la información, se compromete con la implementación de un modelo de seguridad y privacidad de la información en procura de establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de las leyes, la normatividad interna y en concordancia con la misión y visión de la Universidad, en virtud de garantizar la **integridad**, **confidencialidad** y **disponibilidad** de la información institucional, de sus activos de información y de la información de los miembros de su comunidad universitaria.

7.1 Objetivos

La UNIVERSIDAD INDUSTRIAL DE SANTANDER orienta los objetivos del Modelo de Seguridad y Privacidad de la Información[i] a la protección de la información física y digital, buscando alcanzar altos

[5] IVE Consultores. Definiciones básicas sobre la norma iso9001:2015. https://iveconsultores.com/vocabulario-iso-9001/. Octubre 20 de 2021

niveles de calidad y excelencia en su quehacer, disminuyendo el impacto generado sobre sus activos por los riesgos identificados de manera sistemática, para garantizar la implementación de los principios de **integridad, confidencialidad y la disponibilidad** de la misma, acorde con las necesidades de los diferentes procesos, servicios, sistemas de información y grupos de interés identificados.

La gestión de la seguridad y privacidad de la información para la Universidad Industrial de Santander estará determinada por los siguientes objetivos:

1. Cumplir con los principios de seguridad de la información y de la función administrativa.
2. Mantener niveles de seguridad que brinden la confianza de los grupos de interés internos (profesores, administrativos, estudiantes) y externos (egresados, pensionados, entes gubernamentales, sector productivo, proveedores y ciudadanía en general).
3. Realizar una gestión integral de riesgos asociados a la información y a sus activos de información.
4. Articular la gestión y preservación de la información con los instrumentos de transparencia y acceso a la información pública, tales como: Inventario de Activos de Información, Índice de Información Clasificada y Reservada, Tablas de Control de Acceso entre otros.
5. Aplicar el ciclo de vida de la información a través de instrumentos archivísticos como las Tablas de Retención Documental TRD y Tablas de Valoración Documental TVD.
6. Apoyar la innovación tecnológica.
7. Realizar los procesos de migración de información que garanticen la disposición ante la obsolescencia tecnológica.
8. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
9. Establecer los roles y responsables para la implementación del Sistema de Gestión de Seguridad de la Información.
10. Fortalecer la cultura de seguridad de la información en la comunidad universitaria.
11. Garantizar la continuidad de los procesos y servicios frente a incidentes.
12. Definir, implementar, operar y mejorar de forma continua un modelo de seguridad, soportado en lineamientos claros alineados a las necesidades de su quehacer, y a los requerimientos regulatorios.

7.2 Lineamientos.

Para el logro de los objetivos propuestos, la UNIVERSIDAD INDUSTRIAL DE SANTANDER establece los siguientes lineamientos para gestionar la seguridad de la información:

1. Toda persona perteneciente a un grupo de interés interno o externo tendrá asignado algún grado de responsabilidad frente a la seguridad de la información.

2. Para proteger la información generada, procesada o resguardada por la Universidad se establecerán controles que mitiguen los riesgos que se generan por los accesos otorgados a quienes integran los grupos de interés externos.
3. Es necesario aplicar controles que mitiguen el uso incorrecto de la información creada, procesada, transmitida o resguardada por la Universidad, de acuerdo con la clasificación de la información de su propiedad o en custodia.
4. Es fundamental proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos.
5. Se debe controlar la operación de los procesos garantizando la seguridad de los recursos tecnológicos y de las redes de datos.
6. Se deben implementar controles de acceso a la información, sistemas, recursos de red y correos electrónicos, teniendo en cuenta los grupos de interés.
7. La seguridad debe ser parte integral del ciclo de vida de los sistemas de información.
8. Los eventos de seguridad deben gestionarse adecuadamente.
9. Es necesario garantizar la continuidad de la operación con base en el impacto que pueden generar los eventos.
10. Se debe garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

7.3 Roles y responsabilidades

La Universidad por medio del Consejo Superior aprobó el acuerdo 034 de 2019 en el cual establece la creación del Comité Institucional de Gestión y Desempeño "*…instancia en la que se discutirán temas referentes con la gestión institucional en el marco del Modelo Integrado de Planeación y Gestión – MIPG…"* entre ellos *"acompañar la implementación del gobierno en línea en lo referente al impacto de éste sobre la gestión documental y de la información.";* además facultad al señor Rector "*cómo máxima autoridad ejecutiva de la Universidad para que defina y adopte los demás aspectos relacionados y con la implementación y operación del Modelo Integrado de Planeación y Gestión – MIPG…"* .

En correspondencia a lo expuesto la Universidad establece mediante el presente documento de políticas de seguridad de la información, que:

El responsable de la seguridad y privacidad de la información de la Universidad será toda persona integrante de algún grupo de interés interno o externo, para una adecuada implementación, adopción y correcta aplicación de los lineamientos contenidos en las políticas, según su rol, acatará lo estipulado en la siguiente tabla de roles y responsabilidades:

Tabla 1. Roles y responsabilidades en la seguridad de la información en la UIS

Roles/Perfiles	Responsabilidades
Rectoría:	1. Proferir las políticas y procedimientos de seguridad y privacidad de la información 2. Gestionar ante el Consejo Superior los recursos e insumos para la implementación de las políticas y procedimientos, para la adecuación de la infraestructura tecnológica y para la disponibilidad del personal necesario relacionado con la seguridad y protección de la información, de conformidad con la reglamentación institucional.
Comité Institucional de Gestión y Desempeño (CIGyD). Será el órgano institucional responsable coordinar la seguridad de la información.	1. Coordinar las fases o etapas que conlleva la implementación y adopción del Modelo de Seguridad y privacidad de la Información. 2. Avalar los lineamientos y documentación relacionada con las emisión o actualización de políticas y procedimientos relacionados con la seguridad y privacidad de la información. 3. Recomendar roles, responsabilidades, personal, mesa técnica, procedimientos y adecuaciones, que se requieran para el funcionamiento adecuado de la infraestructura tecnológica, de conformidad con la reglamentación institucional, que en pro de la seguridad y privacidad de la información. 4. Divulgar a la comunidad universitaria la documentación relacionada con la seguridad de la información, generada al interior del Comité y que impacte de manera transversal a la misma. 5. Acompañar e impulsar el desarrollo de proyectos de seguridad y de acciones que ayuden a proveer una cultura de seguridad de la información y que sean consistentes con los objetivos de la Universidad. 6. Dar lineamientos sobre situaciones o inconvenientes relacionados con la seguridad de la información, en los casos que lo amerite. 7. Conformar mesas técnicas de trabajo que apoyen las actividades del Comité, al igual que las funciones a realizar por las misma. 8. Las demás funciones inherentes a la naturaleza del Comité.
Equipo Gestión de Incidentes de Seguridad de la Información (EGIS)	1. Definir y comunicar los lineamientos para la gestión de los incidentes seguridad de información digital sobre los activos de información críticos. 2. Atender los aspectos relacionados con los incidentes de seguridad digital reportados o detectados velando por que dichos incidentes sean mitigados.
Responsable de Datos Personales:	En el Manual Institucional para el tratamiento de datos personales se estipula el responsable y responsabilidades del tratamiento de los datos personales. A nivel de Seguridad de la información se sugieren funciones como: 1. Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales 2. Tramitar las consultas, solicitudes y reclamos. 3. Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran. 4. Respetar las condiciones de seguridad y privacidad de información del titular.

Roles/Perfiles	Responsabilidades
	5. Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente
División de Planta Física	Implementar controles de acceso y uso, basados en estándares, que permitan fortalecer la seguridad y privacidad de la información en las áreas o espacios físicos que contengan activos de información considerados de importancia para el desarrollo de las actividades misionales.
División de Servicios de Información	1. Velar por la seguridad y privacidad de la información digital procesada, transmitida y almacenada en y desde los recursos y servicios de tecnológicos utilizados para el soporte de los procesos misionales, estratégicos, de apoyo y evaluación institucional que se encuentran bajo la custodia de la DSI. 2. Definir lineamientos, para el uso y cuidado de los activos de información digital que hagan uso de los servicios tecnológicos a cargo de la DSI. 3. Implementar controles de acceso físico y lógico a los activos de información digital que soportan los procesos institucionales.
Dirección de Certificación y Gestión Documental	1. Proponer políticas para la gestión de la información contenida en medios físicos como: papel, archivos, medios electrónicos, fichas.... 2. Definir lineamientos, para el uso y cuidado de los activos de información digital que hagan uso de los servicios tecnológicos a cargo de la DSI. 3. Implementar controles de acceso físico y lógico a los activos de información digital que soportan las actividades institucionales de carácter misional 4. Velar por una adecuada gestión de la seguridad y privacidad de la información física resultante de los procesos institucionales que apoyan la consecución de los objetivos estratégicos y misionales de la Universidad.
Gestión de Talento Humano	Ofrecer capacitación y sensibilización relacionada con temas de seguridad y privacidad de la información.
Dirección de Control Interno y Evaluación de Gestión	Realizar seguimiento y evaluación del cumplimiento de los lineamientos aprobados para la adopción e implementación de la seguridad y privacidad de la información.
Jefes de UAA / Lideres Proceso /	Adoptar e implementar las políticas institucionales relacionadas con la seguridad y privacidad de la información, con los funcionarios, clientes y proveedores de su unidad. Crear o ajustar los procedimientos de su Unidad que sean necesarios para el cumplimiento de las políticas institucionales de la seguridad de la información.

Roles/Perfiles	Responsabilidades
Propietarios de Activos de Información	1. Autorizar y limitar el acceso a la información disponible en los activos bajo su custodia y a su vez velar por el uso correcto de la información accedida. 2. Aplicar y velar por el cumplimiento de los controles que garanticen la disponibilidad, confidencialidad e integridad de la información de los activos
Comunidad Universitaria: interna y externa.	Adoptar, aceptar y cumplir con las políticas relacionadas con la seguridad y privacidad de la información, aplicables según su vínculo o su relación con la institución, propendiendo por mantener la confidencialidad, integridad y disponibilidad de la información

7.4 Alcance/Aplicabilidad

Esta política aplica a toda la comunidad universitaria interna (profesores, administrativos, estudiantes) y externa (egresados, pensionados, entes gubernamentales, sector productivo, proveedores, aliados académicos y ciudadanía en general), a los procesos y las tecnologías de información, incluido el hardware y software de la UNIVERSIDAD INDUSTRIAL DE SANTANDER.

7.5 Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a la totalidad de las políticas de seguridad y los procedimientos que garanticen la aplicación de los principios de confidencialidad, integridad y disponibilidad de la información, so pena de incurrir en violaciones que puedan acarrear consecuencias de carácter disciplinario, penal, administrativo, entre otras, de conformidad con la legislación vigente aplicable.

7.6 Revisión de la política de seguridad de la información

Las políticas de seguridad y privacidad de la información deberán ser conservadas, revisadas, aprobadas y actualizadas anualmente por la Rectoría y el Comité Institucional de Gestión y Desempeño.

7.7 Entrada en vigencia y modificación

La presente política fue aprobada mediante resolución de Rectoría n.° 1674 del 14 de noviembre de 2023 y entra en vigencia a partir de la fecha de expedición.

8 POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Atendiendo al cumplimiento de la política general de Seguridad y Privacidad de la Información, la **UNIVERSIDAD INDUSTRIAL DE SANTANDER**, por medio de su estructura organizacional, garantiza desde sus procesos que lleva a cabo la gestión de riesgos a los activos de información institucional, fomenta la cultura de la seguridad y privacidad de la información en la comunidad universitaria y da cumplimiento a las políticas específicas de seguridad que se declaran a continuación, en virtud de realizar una gestión idónea de la información gestionada de sus activos de información.

De forma complementaria se ha dispuesto del documento Manual de Implementación de las Políticas de Seguridad y Privacidad de la Información, que tienen como propósito orientar el accionar de los miembros de la comunidad universitaria, extendiéndose a aspectos técnicos que contribuyen a la adopción e implementación de los lineamientos declarados en las políticas de seguridad y privacidad de la información.

8.1 ORGANIZACIÓN INTERNA

8.1.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN GESTIÓN DE PROYECTOS

Desde todo tipo de proyecto (investigación, académico, extensión, inversión, gestión) con respaldo institucional, se velará por proteger la integralidad de la información generada durante las diferentes etapas de gestión del proyecto, inclusive su terminación y liquidación. Para ello la UAA gestora del proyecto deberá:

1. Gestionar y conservar la información (tanto física como digital), en concordancia con los lineamientos establecidos en las Tablas de Retención Documental de la Universidad, garantizando los principios de la seguridad de la información: confidencialidad, integridad y disponibilidad.
2. Identificar, analizar y evaluar los riesgos asociados con los principios de la seguridad y privacidad de la información.
3. Identificar posibles amenazas, vulnerabilidades y establecer los controles pertinentes para mitigar los riesgos identificados.

4. Determinar la necesidad de incluir uno o varios objetivos de seguridad de la información acordes con la información que gestionará el proyecto.
5. En los casos que aplique, para los convenios o contractos con entidades externas, tener presente las normas institucionales establecidas a nivel de seguridad de la información por la Universidad, la entidad externa y las disposiciones legales vigentes
6. Generar el expediente con toda la información y almacenarla en el gestor documental definido por la Universidad.

8.1.2 POLÍTICA DE DISPOSITIVOS MÓVILES

La Universidad velará por la protección de la información que se encuentra almacenada en los dispositivos móviles a cargo de la Universidad, para ello establece que:

1. Realizar el registro de control sobre la asignación, salida, baja y traslado de los dispositivos móviles teniendo en cuenta los parámetros y procedimientos estipulados en el manual normativo y procedimental para la administración y control de los bienes muebles de la UIS.
2. Se permite hacer monitoreo de los dispositivos móviles y someterlos a controles en cuanto al tipo y versionado de aplicaciones instaladas. De manera similar, pueden ser limitados a conexión hacia ciertos servicios informáticos que sean considerados no autorizados o maliciosos.
3. Se consideran “usuarios de dispositivos móviles” a quienes por las características de sus funciones asignadas utilizan habitualmente un portátil, smartphone, teléfono móvil, tableta, etc. dentro y fuera de la organización.
4. Los usuarios de dispositivos móviles institucionales harán uso adecuado de los mismos, teniendo en cuenta:
    a. Los equipos con información importante, sensible o crítica, o que cumplan con la clasificación institucional de información clasificada o reservada, no deben ser desatendidos y, en lo posible, deben quedar resguardados bajo llave; en su defecto, establecer un método de bloqueo, reduciendo así los riesgos asociados a lectura de los datos o la extracción de información por personas no autorizadas o mal intencionadas.
    b. La información que reposa en los dispositivos es responsabilidad del servidor que tiene a su cargo el dispositivo móvil, por ende, debe hacer copias de respaldo en forma periódica
    c. En el caso de devolución del dispositivo deberá entregar la información al líder a cargo y eliminar los datos contenidos en el dispositivo.
    d. Tener especial cuidado cuando los equipos se transportan en vehículos, o se utilizan en espacios públicos, hotel, salas de reunión, centros de conferencias y demás áreas no protegidas, para reducir el riesgo de hurto o pérdida.

e. Quienes son usuarios no están autorizados a cambiar la configuración, ni a desinstalar software de los equipos móviles institucionales, únicamente se deben aceptar y aplicar las actualizaciones.
f. Quien tenga a su cargo un equipo no podrá realizar la instalación de programas desde fuentes desconocidas y sin licencia, por ende, se requiere instalar aplicaciones únicamente desde repositorios seguros y previa consulta al área de tecnología.
g. Reducir la acción de códigos maliciosos solicitando en su unidad la instalación de antivirus licenciados, al igual que con los release y services packs de los sistemas operativo, teniendo en cuenta las normas de uso de la red LAN institucional o el catálogo de servicios suministrados por la División de Servicios de Información.
h. Cuando se conectan los dispositivos a redes públicas de datos que no ofrezcan las garantías de seguridad física y lógica necesarias, se incurre en el riesgo de ser víctima de hurto de información; por ende, se debe evitar realizar transacciones o conexiones no seguras con los servicios institucionales.
i. Acudir al equipo de soporte o mantenimiento en caso de que el dispositivo no cumpla con los parches, configuraciones y protecciones de seguridad establecidas.
j. Quienes tengan configurado el correo electrónico institucional en sus dispositivos móviles (Smart phone, tabletas, pc portátil, etc.) deben reportar tan rápido como sea posible la pérdida o robo de los mismos a la División de Servicios de Información.
k. No deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

5. Para quienes tengan autorizado el uso de dispositivos móviles personales con acceso a los servicios e información institucional deben suscribir un Acuerdo de Usuario Final de Dispositivo Móvil, que incluye la renuncia de la propiedad de los datos institucionales. En cualquier caso, se preserva el derecho de la privacidad del propietario del dispositivo.
6. Todos los usuarios de equipos móviles (computadores portátiles, notebooks, PDA, celulares, tablet, etc), incluyendo los de personal externo a la institución, que desean hacer uso de la red inalámbrica institucional deben contar con un sistema de autenticación basando en las normas de uso de la red LAN institucional.
7. La División de Servicio de Información velará por:
    a. Implementar los controles tecnológicos que impidan la conexión a redes y servicios de la Universidad de equipos móviles con sistemas operacionales con modificaciones consideradas inseguras o que ejecuten acciones para vulnerar la seguridad de las comunicaciones.
    b. Proveer los servicios que faciliten la actualización y aseguramiento de los sistemas operacionales y aplicaciones en los dispositivos móviles institucionales.
    c. Monitorear el uso de los servicios y aplicaciones web institucionales accedidos desde dispositivos móviles conectados a la red LAN de datos.
    d. Implementar controles de seguridad en dispositivos móviles para monitorear, alertar y prevenir fugas de información.

8.1.3 POLÍTICA DE TRABAJO EN CASA PARA LA SEGURIDAD DE LA INFORMACIÓN

1. Quienes laboran en la Universidad acogerán las normas, resoluciones o acuerdos emanados por la Universidad para la modalidad de trabajo en casa. Por ende, es su deber leerlas y apropiarlas y, en particular, en lo que atañe a la política en mención, garantizar la seguridad y privacidad de la información por la ejecución en las acciones que implica la modalidad de trabajo en casa, tales como: responsabilidades sobre el tratamiento de la información y uso de los medios de comunicación, sistemas de información, bases de datos y servicios de red institucional.
2. Quienes sean autorizados para realizar trabajo en casa y que requieran acceder remotamente (fuera de las instalaciones de la Universidad) a los recursos y servicios de red institucional a cargo de la DSI deberán acatar los lineamientos expuestos en la política de conexiones remotas.
3. La información institucional producida en trabajo en casa se organizará de conformidad con los lineamientos archivísticos, garantizando que se integre con las series y subseries documentales correspondientes.

8.1.4 POLÍTICA PARA USO DE CONEXIONES REMOTAS

1. Las conexiones por acceso remoto a los servicios informáticos ofrecidos por la Universidad deben estar sujetas a controles y restricciones definidos por la División de Servicios de Información.
2. Las conexiones remotas requieren ser monitoreadas y se emitirán alertas sobre potenciales amenazas internas y externas de acceso no autorizado a la información o recursos.
3. Los usuarios que requieran realizar acceso remoto a los sistemas de información institucional a cargo de la DSI deberán efectuarlo bajo condiciones de seguridad establecidas por la DSI.
4. Los usuarios que requieran hacer conexión remota a los activos de información de misión crítica deben contar con el visto bueno de la DSI.
5. El soporte, mantenimiento y actualización del hardware y software empleado para realizar las conexiones remotas a los servicios institucionales estará a cargo de La DSI.
6. Los funcionarios que utilicen equipos de uso personal o institucional para conectarse remotamente deben garantizar que el equipo cuente con un antivirus licenciado y actualizado o, en su defecto, sí el licenciamiento institucional lo permite, solicitar a su UAA, y ésta a la DSI, la instalación del antivirus, al igual que los release y services packs de los sistemas operativos, teniendo en cuenta las normas de uso de la red LAN institucional o el catálogo de servicios suministrados por la División de Servicios de Información.

7. Quienes tengan roles sensibles y que requieran acceder remotamente a información o sistemas de información institucionales no deberán realizar conexiones desde:
    a. WIFI de uso gratuito o libre,
    b. Equipos de cómputo de uso libre,
    c. Dispositivos que no cuentan con las condiciones mínimas de seguridad como un antivirus o firewall.
8. Las UAA que ofrezcan servicios (local o en la nube) a los cuales se pueden acceder remotamente, requieren implementar controles o herramientas para monitorear, alertar y prevenir fugas de información.
9. Quienes requieran acceder a las estaciones de trabajo de forma remota deben informar a la persona superior inmediata las necesidades de uso pertinente.
10. El software utilitario usado en conexiones remota debe ser licenciado y autorizado por la DSI.
11. La Dirección de Control Interno y Evaluación de Gestión, con asesoría de la División de Servicios de Información, puede auditar las conexiones remotas con el fin de validar la efectividad de los controles implementados para dichas conexiones.
12. Quienes laboran en la Universidad únicamente deben establecer conexiones remotas en computadores previamente identificados y, en ninguna circunstancia, en computadores públicos o de uso compartido, de hoteles o cafés internet, entre otros.

8.2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN RELACIÓN A LA GESTIÓN DEL PERSONAL.

Debido a que los errores humanos normalmente pueden llegar a convertirse en el mayor riesgo para el manejo adecuado de la información, la política de seguridad de la información en relación con la gestión del talento humano va encaminada a dar lineamientos sobre el tratamiento y validez de la información durante todas las fases del proceso de contratación o vinculación de personal.

La Universidad se encuentra comprometida en garantizar la disponibilidad, integridad y confidencialidad de la información a la cual el personal docente, administrativo, contratistas, estudiantes, proveedores y personal externo tienen acceso en virtud de sus actividades misionales o administrativas de apoyo. Para tal fin, la Universidad ejecuta acciones para la validación, formación, concientización del talento humano sobre el uso de la información para reducir los riesgos de hurto, fraude, filtración o uso inadecuado de los activos de información.

8.2.1 Incorporación de la seguridad de la información en las responsabilidades de personas funcionarias y contratistas.

Es menester incorporar las responsabilidades y roles concernientes a la gestión de la seguridad de la información, tanto física como digital, dentro de las funciones y obligaciones a cargo de las personas al servicio de la Institución y contratistas.

8.2.2 Acuerdo de Confidencialidad.

1. Los acuerdos de confidencialidad o de no divulgación de información deben incluir la aceptación de las políticas y lineamientos en Seguridad y Privacidad de la Información y el tratamiento de la información estipulada por la Universidad, en los términos de la Ley 1581 de 2012 y las demás normas que la adicionen, modifiquen reglamenten o complementen, así como el Decreto 1377 de 2013.
2. El acuerdo de confidencialidad o no divulgación lo deben firmar quienes se desempeñan en la parte administrativa y docente, así como quienes reciben el beneficio de ser auxiliar estudiantil y las personas contratistas, como parte de sus términos y condiciones iniciales de trabajo, indistintamente del tipo de vinculación y teniendo en cuenta su rol institucional, estipulando incluso si se considera necesario el periodo de restricción de divulgación de información después de finalizado el periodo contractual o el beneficio otorgado, según el índice de información clasificada o reservada a la cual se tenga acceso.
3. Este documento debe reposar en la unidad académico administrativa contratante, en el expediente contractual para el caso de proveedores o contratistas. Para el caso de personal vinculado laboralmente, el acuerdo reposará en la División de Gestión de Talento Humano en la historia laboral. Para auxiliares estudiantiles la información reposará en la serie documental "auxiliaturas" de cada UAA.
4. Para el caso de personas colaboradoras o terceras (ej. Personas docentes invitadas, personal en pasantías y otras personas) que por su relación con la universidad accedan a información sujeta a reserva también deben firmar un acuerdo de confidencialidad. Dentro de este mismo acuerdo se declarará que conocen y aceptan la existencia de determinadas actividades que pueden ser objeto de control y monitoreo, detallándose las actividades a fin de no violar el derecho a la privacidad ni los derechos de los implicados.

8.2.3 Selección y vinculación de personal a la planta.

La División de Gestión de Talento Humano es la encargada de realizar las siguientes actividades relacionadas con el proceso de vinculación de personal, las cuales son fundamentales para la seguridad de la información:

1. Verificar los antecedentes disciplinarios, fiscales, judiciales y demás que señale la ley, de las personas candidatas a un empleo, de acuerdo con: las leyes, reglamentos y decretos vigentes

y las normas reglamentarias de carácter institucional relativas a los procesos de contratación.

2. Adelantar el proceso de validación de hoja de vida y soportes adjuntos a la misma.
3. Contemplar la necesidad de realizar estudios de seguridad, de acuerdo con el rol a desempeñar, siempre y cuando tenga que gestionar información considerada como crítica o sensible para la Universidad.
4. Tramitar la autorización a la Universidad para el tratamiento de datos personales del personal docente y administrativo, de acuerdo con la Ley 1581 de 2012 y decretos reglamentarios que dictan disposiciones generales de Habeas Data y regulan el manejo de la información contenida en bases de datos personales.
5. Tramitar la firma del acuerdo de confidencialidad o no divulgación y del acuerdo de cumplimiento de las políticas de seguridad y privacidad de la información, por parte del personal docente y administrativo vinculado.
6. Desarrollar capacitaciones sobre la política de seguridad de la información para el personal docente y administrativo de manera que éste se apropie de los principios de las políticas y se reduzcan los riesgos de hurto, fraude, filtraciones o uso inadecuado de la información o de los activos de información.

Las unidades académico administrativa que intervengan en procesos de contratación, deberán:

1. Asegurar que las personas contratistas, proveedoras y auxiliares estudiantiles, que por su relación con la UAA accedan a información o activos de información considerados sensibles, firmen un acuerdo de confidencialidad o no divulgación y un acuerdo de cumplimiento de las Políticas de Seguridad y Privacidad de la Información para con la Universidad, de manera tal que sus actuaciones estén encaminadas a reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o de los activos de información.
2. Hacer personas terceras o colaboradoras (ej. docentes invitados, personal en pasantías y otras personas) -y en los casos que se requiera- firmen un acuerdo de seguridad, en calidad de aceptación a las políticas institucionales, antes de otorgarles acceso a los activos de información que estén sujetos a reserva o confidencialidad.
3. Definir el procedimiento para validar la documentación de la hoja de vida y soportes adjuntos relacionados con el proceso de contratación del personal o contratista que quedará adscrito o prestará sus servicios a la UAA, ejemplo: referencias (personales, labores), calificaciones (académicas o profesionales), documentación de identidad alterna (pasaporte, tarjeta de conducción, libreta militar), entre otros.
4. Fomentar la cultura de seguridad digital y la gestión de riesgos durante el desarrollo de las actividades de las personas al servicio de la Universidad, profesorado y contratistas,

ejecutando jornadas de sensibilización y promulgando la presente política, afianzando así la confianza con la comunidad universitaria.

8.2.4 Términos y Condiciones Laborales

1. Las personas docentes, administrativas, contratistas, estudiantes, proveedoras y externas que tengan vínculos con la Universidad deben cumplir con las políticas y normatividad establecidas en seguridad y privacidad de la información, las cuales deben ser parte integral de los contratos o documentos de vinculación a que haya lugar, estipulando en las obligaciones específicas para garantizar la confidencialidad e integridad de la información.
2. El personal docente, administrativo, contratistas, estudiantes, proveedores y personal externo, durante el proceso de vinculación a la Universidad, deberán recibir inducción sobre las políticas y lineamientos de seguridad y privacidad de la información. Asimismo, deberán cumplir con la reglamentación y normatividad vigente en relación con la propiedad intelectual y derechos de autor.

8.2.5 Responsabilidades de las personas pertenecientes a la comunidad universitaria.

1. Cada integrante de la comunidad universitaria, indistintamente del tipo de vinculación laboral o contractual que tenga con la Universidad, debe firmar un acuerdo de confidencialidad o de no divulgación, que contenga los términos y condiciones que regulan el uso adecuado y permitido tanto los recursos y servicios informáticos, como de la información física y digital según su rol y tareas de desempeño.
2. Cada integrante de la comunidad universitaria, indistintamente del tipo de vinculación, deberá cumplir con los procedimientos, lineamientos, políticas y controles de seguridad y normas vigentes relacionadas con la seguridad y privacidad de la información que sean aplicables a la Universidad, incluyendo las definidas por el Estado o las autoridades competentes.
3. Las personas integrantes de la comunidad universitaria que por su cargo o rol hagan uso de información sensible, asistirán a las capacitaciones y jornadas de educación y formación que programe la Universidad en materia de seguridad de información física y digital, con el fin de adquirir las competencias necesarias para la gestión adecuada de la información y el uso correcto de los recursos y servicios informáticos institucionales.
4. Las personas servidoras de la Institución, profesores, contratistas y demás personas involucradas deben abstenerse de divulgar información confidencial, en forma escrita, verbal o por cualquier otro medio, así como también deberán abstenerse de incurrir en situaciones que pongan en riesgo la seguridad de la información.

8.2.6 Responsabilidades del estudiantado.

1. Quienes realicen actividades de auxiliares estudiantiles en UAA deberán firmar acuerdo de uso y confidencialidad o de no divulgación de la información, en el cual se establezcan las responsabilidades en cuanto al tratamiento, cuidado y confidencialidad de la información, uso de recursos informáticos o servicios de red a los cuales tendrá acceso para el desarrollo de la auxiliatura.
2. Toda persona estudiante deberá acatar los lineamientos de seguridad y privacidad de la información definidos en la ley y en la reglamentación institucional, con el fin de realizar el tratamiento idóneo y responsable sobre la información confidencial, así como de los recursos informáticos institucionales sensibles o de acceso restringido a los cuales pueda llegar a tener acceso en virtud de las actividades que tenga a cargo. Su vulneración acarreará las sanciones disciplinarias a que haya lugar, de conformidad con los reglamentos vigentes.

8.2.7 Responsabilidades de Usuarios Externos

1. Los usuarios externos que procesan o almacenan información, a la que requieren tener acceso para cumplir con las obligaciones contractuales previas adquiridas con la universidad, deben aceptar por escrito los términos y condiciones de uso de la información y de los recursos informativos que gestionan.
2. También, deberán asistir a las jornadas de sensibilización o concientización sobre el uso responsable de la información o de los recursos informáticos puestos a disposición para el desarrollo de sus actividades contractuales.
3. Para evitar conflictos de responsabilidades, los usuarios externos que requieran tener o mantener una cuenta de correo con el dominio @uis.edu.co o con el dominio @correo.uis.edu.co no tendrán acceso a las listas de correos institucionales.

8.2.8 Entrenamiento, concientización y capacitación

1. Las personas funcionarias deben ser entrenadas y capacitadas en la gestión responsable de la seguridad y privacidad de la información, de las instalaciones de procesamiento de información y de los recursos tecnológicos informáticos requeridos en el desarrollo de sus funciones y actividades laborales. Esto con el fin de sensibilizarlas sobre la protección adecuada de los recursos y la información de la Universidad. Asimismo, se debe garantizar la comprensión del alcance y contenido de las políticas y directrices de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente e integral desde su función.
2. Las personas pertenecientes a grupos de interés externos que requieran tener acceso a información institucional, a instalaciones de procesamientos de información o a recursos

tecnológicos informáticos necesarios para el desarrollo de sus funciones y actividades contractuales deben recibir una adecuada sensibilización en materia de las políticas, normas y procedimientos de Seguridad y privacidad de la Información que tiene la Universidad.

3. La División de Gestión de Talento Humano, con asesoría de la División de Servicios de Información, se encargará de incluir en su plan de capacitación actividades relacionadas con seguridad de la información, que propendan por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.
4. La Dirección de Certificación y Gestión documental, con asesoría de la División de Servicios de Información, emitirá lineamientos de buenas prácticas para la administración de archivos físicos y digitales ubicados en las estaciones de trabajo de los funcionarios, al igual para la gestión de la información digital almacenada en las bases de datos o accedida desde los servicios informáticos considerados de misión crítica.
5. La División de Servicios de Información se encargará de emitir lineamientos a los funcionarios sobre amenazas de seguridad informática detectadas en la red de datos institucional, que puedan poner en riegos la información almacenada en las estaciones de trabajo, servidores o activos de información de misión crítica.

8.2.9 Desvinculación, licencias, vacaciones o cambio de labores de personas funcionarias y personal provisto por terceros.

1. Cuando una persona funcionaria o contratista finalice su proceso de vinculación laboral o contractual, o cambie de rol, deberá hacer entrega a la persona responsable de la UAA o a quien le prosigue, según sea el caso, de:
    a. la información generada en el desarrollo de sus actividades durante el periodo de vinculación.
    b. Los activos de información bajo su responsabilidad.
    c. Los datos de las credenciales de acceso suministradas para el acceso a los servicios de red.
2. La persona encargada de una UAA a la cual se encuentra adscrito alguien vinculado a la UIS que cambie de rol, se encuentre en proceso de licencia o esté disfrutando vacaciones notificará a la unidad competente para que realice el retiro temporal o definitivo de los servicios y activos informáticos a los que tenía acceso o, en su defecto, la reasignación de los nuevos accesos por el cambio de rol.
3. Cuando el personal se desvincula de la Universidad, quien esté encargado de la UAA a la cual se encontraba adscrito solicitará a la DSI, de manera inmediata, la inactivación o revocación de los permisos de acceso sobre los servicios informáticos institucionales a los cuales tenía acceso para el desarrollo de sus funciones.
4. A las personas externas, naturales o jurídicas, que tengan acceso a información o a las instalaciones de cómputo en las que se procesa, almacena o genera información se les

retirarán los permisos y credenciales de acceso una vez finalicen el periodo de las actividades contractuales. La persona a cargo del trámite correspondiente será aquella que dirige la UAA que solicitó la vinculación o en la que se realizaron las actividades.

5. La persona a cargo de alguna UAA que celebre contratos o convenios establecerá en los acuerdos de confidencialidad, y cuando haya lugar, una cláusula en la cual se indique la prohibición de divulgar información después de finalizado el periodo contractual, teniendo a su vez en cuenta la clasificación de la información estipulada en el índice de información clasificada y reservada, las tablas de control de acceso y los activos de información institucional.

8.2.10 Procesos disciplinarios.

Los procesos disciplinarios se encuentran regulados en la ley y en la normatividad Institucional, en virtud de los sujetos disciplinables a los que se dirigen, ya sean servidores públicos o estudiantes, por lo tanto, en los eventos en que se configure alguna vulneración o incumplimiento de las políticas, reglamentación o normatividad, que atente contra la seguridad de la información de la Universidad o la protección de datos personales de los miembros de la comunidad universitaria, se adelantarán las indagaciones y se desarrollarán los procedimientos a que haya lugar, de conformidad con lo dispuesto en la normativa vigente aplicable a la materia.

8.3 GESTIÓN DE ACTIVOS DE INFORMACIÓN DE SEGURIDAD DIGITAL

La Universidad por medio de sus Unidades Académico Administrativas (UAA) y líderes de proceso realizará la gestión correspondiente para el levantamiento del inventario de sus activos de información de seguridad digital, ya sean de índole físico o lógico velando por su disponibilidad, integridad y confidencialidad.

8.3.1 Generalidades

1. Los recursos tecnológicos son propiedad de la Universidad Industrial de Santander, su clasificación y gestión se realiza teniendo en cuenta los procedimientos definidos por la Sección de Inventarios en el manual normativo y procedimental para la administración y control de los bienes muebles de la UIS.
2. Todos los recursos tecnológicos físicos de las UAA deben ser inventariados y asignados a un funcionario responsable quien se convertirá en el custodio del mismo y velará por su uso y cuidado mientras lo tenga a su cargo.

3. Las UAA que dispongan de recursos tecnológicos digitales como bases datos, software, aplicativos y plataformas, que por su importancia son sensibles para la gestión de la información, deberán incluirlos en el inventario de activos de información digital.
4. Cuando un activo es considerado de información, ya sea físico o digital, será inventariado y clasificado por la UAA teniendo en cuenta la metodología para el levantamiento de activos de información digital.
5. Los miembros de la comunidad universitaria son responsables de hacer buen uso de los recursos tecnológicos de la Universidad y de la información que se almacena y procesa por medio de ellos. En ningún momento estos recursos o información pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros funcionarios, colaboradores o terceros, legislación vigente, políticas y lineamientos de seguridad de la información establecidas por la Universidad.
6. Todas las UAA deben generar un inventario de activos de información digital y actualizarlo una vez al año, siguiendo las directrices del documento: "Lineamientos para la creación y actualización del Inventario de Activos de Información". Para el caso de la información física considerada como clasificada o reservada se seguirán los lineamientos definidos por la Dirección de Certificación y Gestión Documental en las Tablas de Control de Acceso y el Índice de Información Clasificada y Reservada.
7. Los funcionarios deben velar por el funcionamiento adecuado del recurso asignado y en caso de detectar falencias solicitar el soporte a las dependencias internas correspondientes (División de Servicios de Información o Dirección de Mantenimiento Tecnológico) siguiendo el procedimiento para la prestación de servicios de tecnologías de información según la necesidad, o en su defecto acudir al servicio de garantía o al servicio de soporte externo contratado.
8. El catálogo de servicios de la División de Servicios de Información contiene la lista de recursos informáticos disponibles por esta unidad para el servicio y uso de las UAA o sus funcionarios.
9. La DSI elaborará los instructivos, procedimientos o guías necesarios para establecer los lineamientos técnicos de la implementación de la política de seguridad de la información en relación a los activos de información que estén bajo su custodia y administración.
10. Todo miembro de la comunidad universitaria, que tenga asignado un equipo tecnológico de propiedad de la universidad, debe entregarlo al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos móviles o removibles.
11. Los activos de información digital institucionales que estén bajo custodia de la DSI deberán gestionarse bajo los lineamientos técnicos establecidos por la DSI.
12. Los activos de información de tipo documental deben organizarse según los instructivos, procedimientos o guías institucionales construidas para la organización de los archivos de gestión y la transferencia documentales según lo establecido en las TRD.

13. Los activos de información que permiten la consulta y reproducción de la información física y digital deben contar con el mantenimiento adecuado que garantice su uso adecuado y permanente.
14. Los activos de información físico o digital se encuentran sujetos a auditorías por parte de la Dirección de Control Interno y Evaluación de Gestión.
15. La División de Servicios de Información puede realizar monitoreo sobre los activos de información digital institucional sin que esto identifique a un usuario en particular. Este procedimiento se podrá llevar a cabo siempre y cuando se tengan indicios de su vinculación a un incidente de seguridad.
16. En las áreas en donde se tenga equipos de procesamiento de información, no se permitirá fumar, tomar ningún tipo de bebidas o consumir alimentos.

8.3.2 POLÍTICA PARA LA GESTIÓN DE CENTROS DE PROCESAMIENTO Y DE CABLEADO.

1. Los centros de cómputo o áreas que la universidad considere como críticas contarán con elementos detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo indicio de incendio. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses dejando los respectivos registros de los resultados de las pruebas.
2. Disponer de extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipo eléctrico o electrónico, papel o químicos especiales.
3. Las áreas de procesamiento o de conectividad crítica deben disponer de las condiciones ambientales de temperatura, humedad, conectividad e iluminación para un funcionamiento adecuado, las cuales serán monitoreadas de forma permanente manteniendo un registro de las mismas.
4. La Universidad dispondrá de por lo menos dos centros de datos (principal y secundario) los cuales deberán contar con tecnología de replicación periódica que permitan la redundancia.
5. Sólo personal autorizado por la DSI podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información clasificada como de misión crítica, siguiendo los lineamientos de conectividad y esquema de seguridad establecidos por la DSI.
6. El cableado de la red debe ser protegido de interferencias usando canaletas que lo protejan.
7. Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
8. A los centros de datos o infraestructura de red sobre la cual funcionan estos centros de datos, se les debe implementar sistemas redundantes de alimentación eléctrica de manera tal que permitan soportar el funcionamiento de las operaciones de los servicios críticos de actividad misional mientras se restaura el suministro de energía.

8.3.3 POLÍTICA USO DE LOS SISTEMAS DE INFORMACIÓN

1. El sistema de seguridad definido por la División de Servicios de Información para los diferentes sistemas de información que apoyan la gestión de la Universidad Industrial de Santander está basado en la estructura de roles – usuarios.
2. Los roles se establecen en cada una de las unidades académico administrativa, UAA, responsables de cada sistema (propietario/dueño del activo de información). Ejemplo: División de Financiero es propietario del sistema de información financiero; la Dirección de Admisiones y Registro Académico es propietario del sistema de información académico.
3. Los responsables de los sistemas de información deben hacer firmar un acuerdo de confidencialidad o no divulgación y de no repudio a los funcionarios a quienes les autoricen el acceso a los mismos.
4. El desarrollo, mantenimiento, cambio y actualización de los sistemas de información institucionales es solicitado por la UAA responsable del sistema y será ejecutado, dependiendo su viabilidad, por los líderes funcionales de la División de Servicios de Información, quien tiene la custodia de los mismos. Las actividades en mención se llevarán a cabo de acuerdo al procedimiento definido para la elaboración, mantenimiento de software y procesamiento de datos.
5. Los usuarios no pueden realizar copias de los sistemas de información institucionales que se encuentren instalados en los equipos para su distribución.
6. Los usuarios no deberán modificar, revisar, transformar o adaptar, descompilar o realizar ingeniería inversa a cualquier software o sistema de información de propiedad de la Universidad.
7. Los usuarios no pueden realizar copias de la información que arrojan los sistemas de información institucionales para distribuirlas a otros funcionarios que no la requieren para el desarrollo de sus funciones, o a entes externos, sin previa autorización del responsable del activo de información. La distribución de esta información puede llegar a ser usada en contra de otros miembros de la comunidad o de la misma Universidad, e incluso al ser divulgada puede ser utilizada con fines delictivos incurriendo el usuario del sistema de información en violación de las políticas de seguridad y privacidad de la información de datos personales.
8. Los usuarios de los sistemas de información deberán informar a la DSI sobre cualquier mal funcionamiento, violación de las políticas de seguridad y privacidad, uso indebido y debilidades de seguridad de la información sobre los sistemas de información institucionales.
9. El líder funcional de cada una de las aplicaciones institucionales que se encuentran bajo la custodia de la DSI, tiene la responsabilidad de administrar el aplicativo o delegar dicha función, pero no la responsabilidad, en la persona que lo considere pertinente.

8.3.4 POLÍTICA USO DE SOFTWARE Y LICENCIAS

1. Los usuarios deberán utilizar únicamente el software legalmente adquirido por la UAA o por la Universidad, o el que forme parte de los diferentes tipos de

licenciamiento suscritos de forma institucional abarcando a los miembros de la comunidad universitaria, previa aceptación de los términos y condiciones de uso.

2. La administración (adquisición, renovación, distribución) de licencias software que formen parte de los diferentes convenios de software destinados al uso general de la Universidad, estarán bajo la custodia de la DSI quien controlará el número de licencias instaladas en relación a las adquiridas.
3. La DSI emitirá, por lo menos una vez al año, la lista actualiza del software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios.
4. Los usuarios de las UAA podrán realizar en sus estaciones de trabajo: instalaciones, desinstalaciones, renovaciones o actualizaciones de software, siempre y cuando el software haya sido adquirido legalmente por su UAA o la Universidad; o en su defecto solicitar el apoyo a la División de Servicios de Información.
5. Los usuarios no pueden realizar copias de software que se encuentre instalado en los equipos para su distribución.
6. Los activos de información físico o digital se encuentran sujetos a auditorías por parte de la Dirección de Control Interno y Evaluación de Gestión.
7. La Dirección de Control Interno y Evaluación de Gestión podrá auditar en cualquier momento el software utilizado en cada UAA.
8. La descarga, instalación o uso de aplicativos, programas informáticos, software no autorizado será considerado como una violación a las Políticas de seguridad y privacidad de la información de la Universidad
9. En caso de presentarse algún tipo de reclamación por software ilegal, la responsabilidad recaerá sobre el usuario responsable del dispositivo en donde se encontrase instalado dicho software.
10. Los usuarios que requieran instalar, hacer uso o compartir software (libre o propio) en los equipos institucionales, asumirán la responsabilidad y consecuencias respectivas sobre los efectos de las acciones que resulten de la instalación o uso del software instalado.
11. Todo miembro de la comunidad que se entere de cualquier uso indebido o no autorizado de software o la documentación vinculada a estos, deberá comunicarlo a la División de Servicios de Información o la Dirección de Control Interno y Evaluación de Gestión.
12. El software siempre deberá ajustarse a los términos de uso y licenciamiento establecidos por el fabricante, incluidas las versiones de prueba.
13. Está autorizado el uso de software de terceros, siempre y cuando la UAA realice el proceso de licenciamiento respectivo.
14. No está autorizada la reproducción de programas de software y la documentación vinculada a éste, excepto con fines de respaldo.
15. Ante cualquier duda referente a los términos de licenciamiento o legalidad de un software, los funcionarios pueden consultar a la DSI.
16. El usuario responsable del dispositivo deberá desinstalar o desactivar las licencias que hayan caducado, ya sea porque finalizó el periodo de licenciamiento asignado y no fue solicitada su prorroga de uso o por cualquier otra situación que impida su instalación o uso.

17. Se prohíbe el uso de programas o aplicaciones que permitan accesos no controlados a los activos informáticos institucionales, sin la autorización previa de la DSI.

8.3.5 POLÍTICA PROTECCIÓN Y USO DE LAS ESTACIONES CLIENTE DE TRABAJO

1. El funcionario aceptará los equipos de cómputo que se le han asignado y a partir de ese momento será responsable de los equipos y accesorios que le han sido entregados, de su cuidado y su buen uso. La aceptación se hará por medio del sistema de información.
2. La DSI prepara las estaciones de trabajo fijas y/o portátiles de los funcionarios dejándolas a punto con el hardware y software básico configurado y requerido para su funcionamiento de acuerdo a los diferentes tipos de licenciamiento institucional.
3. Las estaciones de trabajo deberán permanecer con los programas y configuraciones bases de seguridad instaladas por la DSI, tales como: el sistema operativo, office, antivirus, firewalls; por ende, los funcionarios no deben desinstalar o alterar dichas configuraciones o programas.
4. Es responsabilidad de los usuarios mantener el software actualizado en todos los equipos que utilice y conecte a la red de datos institucional, tales como:
    a. bases de datos de los anti-virus, anti-malware, firewalls, entre otros,
    b. Releases, services packs de los sistemas operativos.
5. Si un funcionario recibe un equipo de cómputo institucional sin antivirus o antivirus desactualizado deberá acudir a la DSI para la respectiva instalación o actualización.
6. El uso de dispositivos como unidades de almacenamiento USB, CD o cualquier otro, es de exclusiva responsabilidad de los usuarios, los cuales deberán asegurarse de que estos no contengan ningún medio de contaminación de virus.
7. Los usuarios no deberán alterar el contenido físico o lógico de las estaciones de trabajo, tales como configuración, conexiones de red, direccionamiento IP, extracción o traslado de hardware, usuarios locales de la máquina, papel tapiz, protector de pantalla institucional, entre otros. Estos cambios podrán ser realizados únicamente por la unidad de soporte técnico autorizado.
8. La información a almacenar en las estaciones de trabajo deberá gestionarse siguiendo los lineamientos definidos en la "política sobre almacenamiento".
9. Los usuarios son responsables de realizar las copias de respaldo de la información almacenada en los equipos que utilizan para el desarrollo de sus labores.
10. Si un equipo de cómputo requiere seguir algún procedimiento de formateo o reinstalación de aplicaciones, por problema de infección de virus, o por algún daño que haya sufrido, se debe realizar una solicitud a la Mesa de Servicios de Tecnología.
11. Las estaciones de trabajo o recursos tecnológicos que no requieran ser usados en horas no laborales, deben permanecer apagados, e incluso cuando el funcionario requiera ausentarse por largos periodos de tiempo de su puesto de trabajo.
12. Es responsabilidad del usuario o funcionario evitar en todo momento la fuga o pérdida de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

13. En lo referente a la ubicación de computadores y hardware en general, se debe tener especial cuidado contra fallas del sistema de control del medio ambiente y otras amenazas que puedan afectar la normal operación de los elementos.
14. Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música y fotos que no sean de carácter institucional.
15. Los usuarios no deben almacenar información de tipo laboral, institucional o personal, en los computadores de aulas de clase, aula móvil, biblioteca, salas de computadores, computadores de préstamo y laboratorios.
16. Cuando un equipo vaya a ser retirado de servicio debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento de la información de manera tal que no sea recuperable y si es llegado el caso se debe perforar los discos duros para evitar la recuperación de la información y uso indebido de la misma.
17. Para las estaciones de trabajo que se quieran reasignar a otro funcionario, donar o sacar de las instalaciones de la universidad, el usuario responsable del equipo, en primera instancia, debe garantizar que en dichos elementos no se encuentra información personal o institucional clasificada de acuerdo a los niveles de clasificación de la información, o en su defecto se debe eliminar toda información residente en los discos de manera tal que no sea recuperable.
18. Los usuarios que requieran trasladar equipos de cómputo fuera de su ubicación de trabajo tener presente:
    a. No dejarlos desatendidos en espacios que no cuenten con medidas de seguridad.
    b. Transportarlos siguiendo las recomendaciones del fabricante.
19. Cualquier empleado de la Universidad que sea responsable de un contrato institucional en el cual se involucren computadores, servidores y periféricos, de propiedad de un tercero, debe solicitar autorización a la UAA responsable del contrato para el uso de éstos dentro de las instalaciones de la Universidad, y debe garantizar que se establezcan los términos y condiciones de su uso, en el contrato. Adicionalmente, debe cumplir con la política institucional de conectividad a la red de datos.
20. Los elementos de las estaciones de trabajo (CPU y pantallas) se conectarán a la red de energía regulada de los puestos de trabajos; los otros elementos deberán conectarse a la red no regulada.
21. En caso que se requiera compartir información sensible entre varios funcionarios, ya sea de forma temporal o permanente, se recomienda crear perfiles para cada usuario, asignando un funcionario responsable que garantice la realización de copias de seguridad y la creación de los perfiles para cada uno de los usuarios.
22. Si un funcionario requiere facilitar el uso de su equipo de cómputo a otro funcionario, se recomienda crear un usuario con el perfil de invitado.

8.3.6 POLÍTICA PARA ADMINISTRACIÓN DE SERVIDORES Y BASES DE DATOS.

1. La Universidad dispone de una infraestructura de servidores en la cual almacena información sobre bases de datos, sistemas de información, desarrollos, e información considera crítica para varios procesos que respaldan las actividades de apoyo misional de la Universidad.
2. La División de Servicios de Información, por medio de líderes funcionales, es la unidad responsable de administrar el funcionamiento de los servidores y bases de datos considerados de misión crítica.
3. Los funcionarios responsables de administrar servidores, bases de datos o servicios instalados en ellos, son los primeros responsables en mantener velar y mejorar su funcionamiento incluyendo la respectiva seguridad contra accesos malintencionado estableciendo lineamientos de configuración en los servicios o servidores.
4. Los administradores de base de datos de la División de Servicios de Información tendrán un único usuario con privilegios "DBA" sobre cada una de las bases de datos institucionales de la Universidad.
5. Los administradores deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro.
6. Solo personal autorizado por la División de Servicio de Información podrá instalar software o hardware en los servidores e infraestructura de telecomunicaciones sobre los cuales funcionan estos servidores.
7. Los administradores deben monitorear el funcionamiento de los servicios e identificar anomalías en cada uno de los servidores y bases de datos generando un consolidado de amenazas identificadas.
8. Los servidores y servicios en los que esté presente la marca UIS deben establecer un lineamiento de actualización periódica (ejemplo: mensual, trimestral, semestral u otro) sobre las versiones de los componentes de los diferentes sistemas de seguridad operativos, incluidos motores de detección, bases de datos de firmas, software de gestión en el lado cliente y servidor, etc.
9. Para los servidores que cuenten con sistemas operativos próximos a salir del periodo de soporte por parte del fabricante se les debe analizar la viabilidad de actualizarse a versiones más recientes
10. Los administradores por defecto deben bloquear, todos los protocolos, puertos y servicios que no se requieran en los servidores. Los servidores se deben configurar con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.
11. Los administradores de servicios que soliciten aperturas de puertos a la administración de la red LAN institucional, están en la obligación de sustentar sus requerimientos para que a través de un análisis se establezca el nivel de Riesgo y de Impacto.
12. Las UAA que dispongan de servidores conectados a la red LAN deberán implementar endurecimiento (hardening) en sus servidores a nivel del sistema operativo para limitar puertos, número de conexiones y aplicar buenas prácticas de seguridad según la función del servidor. En caso de no contar con personal capacitado se sugiere contratar un servicio especializado. Posteriormente, deben informar al administrador de la

red LAN institucional sobre las políticas de hardening que se debe aplicar a nivel de red para estos servidores o servicios.

13. Las UAA que instalen o liberan servicios desde servidores propios o institucionales deben definir un responsable (administrador) del servicio e incluso del servidor. Esto con el fin de no dejar servicios o maquinas sin un responsable de su funcionamiento o seguridad.
14. Los administradores de servidores bajo control directo de la DSI y que sean de misión crítica, deben tener identificado los servicios publicados y puertos TCP/UDP en los servidores hacia la LAN y la WAN
15. La información de los servidores principales es respaldada en cintas y servidores alternos y podrá ser recuperada en caso de un desastre o incidentes de seguridad.
16. La información trasladada de los servidores de producción a los servidores de prueba cuenta con los mismos controles de acceso que se aplican sobre los datos de producción.
17. Las acciones del DBA y/o administrador de servidores, o usuarios con permisos privilegiados deben ser revisadas y auditadas de forma ocasional.
18. Solo personal autorizado podrá realizar actividades de administración remota sobre los servidores, bases de datos o infraestructura de procesamiento de información sobre la cual funcionan estos activos, utilizando el esquema de seguridad definido por la División de Servicios de Información.
19. Para los servidores que se les desea dar de baja o saldrán de las instalaciones de la Universidad, se debe garantizar que en dichos elementos no se encuentre información clasificada de acuerdo a los niveles de clasificación de la información, o en su defecto aplicar las políticas definidas para el borrado seguro.
20. Los servidores deben estar conectados a una red de energía regulada.
21. Las UAA con servidores o subdominio bajo el dominio institucional uis.edu.co deben velar por el cumplimiento de los lineamientos mencionados en esta política y deberán responder por cualquier incidente de seguridad que se presente en sus servidores.

8.3.7 POLÍTICA DE SOPORTE Y MANTENIMIENTO DE RECURSOS Y SERVICIOS INFORMÁTICOS.

1. Todo funcionario podrá acceder al servicio de soporte y mantenimiento tecnológico ofrecido por la División de Mantenimiento Tecnológico o la División de Servicios de información, siempre y cuando el equipo que requiera el soporte sea de propiedad de la Universidad.
2. La División de Servicios de Información suministra el soporte respectivo sobre los servicios estipulados en su catálogo de servicios divulgado en la página web de la universidad.
3. La Universidad dispone de un aplicativo informático para que los funcionarios registren las solicitudes de tipo de mantenimiento requerido, el cual será gestionado posteriormente por la mesa de ayuda.
4. La UAA deberá contar con una bitácora sobre las acciones correctivas aplicadas sobre los equipos que han sido intervenidos por los técnicos de soporte.

5. Los funcionarios que brinden el servicio de soporte técnico deben registrar las acciones sobre el tipo de mantenimiento y actividades ejecutadas sobre el equipo atendido.
6. En cuanto a los equipos de misión crítica que requieren soporte por personal externo deben contar con una bitácora sobre las acciones preventivas o correctivas aplicadas sobre los mismos por parte de los proveedores.
7. No se prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de propiedad de la Universidad.
8. Las actividades de mantenimiento sobre los activos de información, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser programadas e informadas con anticipación a la comunidad universitaria.
9. Las UAA deben mantener contratos de soporte y mantenimiento de los equipos críticos a su cargo.
10. Solo personal con la idoneidad respectiva pueden realizar tareas de mantenimiento, revisión de software, recuperar datos perdidos o eliminar software malicioso.

8.4 POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

8.4.1 Generalidades

1. La Universidad Industrial de Santander, por medio de la Dirección de Certificación y Gestión Documental, emite directrices para que la información que utilizan, generan o procesan las UAA o dependencias sea tratada y protegida adecuadamente; para ello, establece los niveles más adecuados de clasificación de acuerdo con los requisitos legales, criticidad, susceptibilidad y divulgación no autorizada permitiendo que los propietarios de la misma apliquen y ejecuten los controles requeridos para su protección.
2. Las UAA deben generar un inventario de todos los activos de información para los procesos que lideran, así como su clasificación de acuerdo con la Guía para la clasificación de los activos de Información establecida, la cual está basada en las Tablas de Retención Documental de la Universidad. Para el caso del levantamiento o actualización del inventario de activos informáticos/tecnológicos de información se requiere basarse en la metodología y guía definidas.
3. La información, así como los activos donde ésta se almacena o procesa, deben ser asignados a un responsable, inventariados y clasificados para darles una adecuada protección. Los propietarios de los activos de información deben llevar a cabo la actualización del inventario al interior de sus procesos o áreas, con frecuencia anual.
4. La información física y electrónica de las Unidades o dependencias deben tener un período de almacenamiento que puede ser dictaminado por requerimientos legales o misionales. Este período debe ser indicado en las tablas de retención documental y cuando se cumpla su período de retención debe aplicarse su disposición final de acuerdo con la normatividad aplicable.

5. Los miembros de la comunidad (profesores, administrativos, empleados, estudiantes) deben tener en cuenta estas consideraciones y las expuestas a continuación cuando impriman, escaneen, saquen copias, envíen faxes o emails.

8.4.2 Esquema de Clasificación de la Información

1. La Dirección de Certificación y Gestión Documental será el órgano encargado de definir las directrices para la clasificación de la información y las medidas de tratamiento o de manejo que deben dársele a la información en función del nivel de clasificación al que pertenecen: público, clasificado, uso interno, reservado u otro.
2. Para el manejo y almacenamiento de la información acorde a la clasificación que se establezca es necesario tener en cuenta lo siguiente:
    a. Ejecutar los lineamientos definidos para la organización documental de la información institucional.
    b. Restringir el acceso solo al personal debidamente autorizado.
    c. Mantener un registro formal de los receptores autorizados de datos o información.
    d. Conservar los medios de almacenamiento en un ambiente seguro.
3. Para el caso de los activos de información digital seguir el esquema definido en la guía de levantamiento de activos de información

8.4.3 Etiquetado y manejo de Información

1. La tecnología utilizada para salvaguardar, facilitar y conservar la información de los documentos en soportes informáticos debe garantizar la seguridad de no permitir alteraciones o consultas de personas no autorizadas, teniendo en cuenta los lineamientos definidos en la guía para protección y conservación de archivos.
2. El etiquetado o rotulado de la información deberá seguir los lineamientos definidos por la Dirección de Certificación y Gestión Documental colocando en un lugar visible el tipo de clasificación asignada al documento: reservada, clasificada, pública u otro.
3. La información almacenada en medios magnéticos se deberá inventariar, anexando la descripción y las especificaciones de la misma, clasificándola y etiquetándola en los mismos niveles establecidos en clasificación de la información.
4. Ningún miembro de la comunidad o tercero deberá poseer material o información confidencial de la Institución para usos no propios de su responsabilidad.
5. La Dirección de Certificación y Gestión Documental recibirá las transferencias documentales de acuerdo con el calendario anual de transferencias documentales.
6. Es responsabilidad de los funcionarios en materia de manejo de la información:
    a. Acatar los lineamientos de la Guía de Clasificación de la Información, emanada por la Dirección de Certificación y Gestión Documental, para el acceso, divulgación, almacenamiento, copia, transmisión, conservación, etiquetado y eliminación de la información contenida en los recursos tecnológicos.

b. Impedir el acceso no autorizado a información impresa, digitalizada o almacenada en puestos de trabajo cuando quedan desatendidos.
c. Identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que ésta pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.
d. No dejar expuestos documentos con información confidencial o con datos personales en el momento de usar los servicios de impresión, escaneo, fotocopiado o envío de fax, para evitar su divulgación no autorizada.
e. Mantener los puestos trabajos libres de documentos y medios de almacenamiento utilizados para el desempeño de las labores cuando se finaliza la jornada laboral.
f. Aplicar los controles de seguridad definidos por la política de seguridad y privacidad de información de la Universidad para la preservación de la confidencialidad, integridad y disponibilidad de los activos de información tanto en estaciones de trabajo como en ambientes de procesamientos en nube de datos.
g. Mantener organizado el archivo de gestión, acatando los lineamientos establecidos por la Dirección de Certificación y Gestión Documental.

7. Es responsabilidad de los jefes de UAA, área o dependencia o de quién haga sus veces:
   a. Velar por la organización, consulta, conservación y custodia de la documentación física y electrónica del archivo de gestión de su Unidad.
   b. Establecer mecanismos para el control de la reprografía de los documentos, con el fin de mantener la integridad y confidencialidad de la información.
   c. Transferir al archivo central la documentación en forma ordenada y organizada, de acuerdo con los tiempos de vigencia estimados en la Tabla de Retención Documental de la Universidad, acompañada del documento formato utilizado para realizar las transferencias documentales.
   d. Utilizar los medios estipulados para realizar adecuadamente la disposición final de la documentación física y electrónica con base en lo establecido y dispuesto en las Tablas de Retención Documental de la Universidad, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.
   e. Realizar la entrega de la información conveniente a quien lo suceda en el cargo.
   f. Resguardar la información almacenada en medios magnéticos de carácter histórico; está quedará documentada como activo del área.
   g. Custodiar los documentos y enviarlos a la Dirección de Certificación y Gestión Documental, según lo especificado en las tablas de Retención Documental.
   h. Delimitar las responsabilidades de sus subordinados y determinar quién está autorizado a efectuar operaciones emergentes con la información considerada sensible, tomando las medidas de seguridad pertinentes.

8.4.4 Administración de los Archivos

1. Los funcionarios de la Universidad al desvincularse de las funciones o actividades titulares entregarán los documentos y archivos a su cargo debidamente organizados e inventariados.

2. Es deber de todo funcionario de la Universidad custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
3. A todo funcionario de la Universidad le está prohibido:
    a. Omitir, retardar o no suministrar debida y oportuna respuesta a las peticiones, así como retenerlas o enviarlas a un destinatario que no corresponde o que no esté autorizado.
    b. Ocasionar daño o dar lugar a la pérdida de expedientes, documentos o archivos que hayan llegado a su poder por razón de sus funciones/actividades.
    c. Dar lugar al acceso o exhibir expedientes, documentos, información o archivos a personas no autorizadas.
    d. Realizar actividades tales como borrar, alterar o eliminar información de su Unidad, dependencia o de la Universidad de manera malintencionada.
    e. Extraer documentos hacia el exterior de la Universidad sin autorización del jefe de la UAA o de la dependencia.

8.5 GESTIÓN DE MEDIOS DE ALMACENAMIENTO.

Los lineamientos de estas políticas propenden por proteger la información de la Universidad velando por la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento:

8.5.1 POLÍTICA PARA GESTIÓN Y DISPOSICIÓN DE MEDIOS REMOVIBLES

1. Por anticipado a los lineamientos de esta política se aclara que la información puede estar almacenada o transportada tanto en formato digital en dispositivos o unidades de almacenamiento removibles como CD, DVD, Flash USB, discos magnéticos, discos duros, tarjetas de memoria, cámaras fotográficas, cámaras de video, celulares, entre otros; como en formatos tradicionales tales como el papel, microfichas, películas, etc.
2. Al momento de la emanación de esta política no está restringido el uso de dispositivos y unidades de almacenamiento removibles como los mencionados previamente, pero el uso adecuado y controlado de estos medios para transportar o salvaguardar información recae sobre los usuarios haciéndose responsable de cualquier incidente de seguridad de la información en contra de la Universidad o de cualquier miembro de la comunidad universitaria.
3. Los medios y equipos donde se almacena, procesa o comunica la información deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento y estar almacenados en un ambiente seguro acorde con las especificaciones del fabricante.

4. Toda la información clasificada como CONFIDENCIAL o RESERVADA que sea almacenada en medios removibles requiere de protección especial y deberá ser almacenada de forma segura incluyendo el dispositivo utilizado para su almacenamiento. Será responsabilidad del funcionario el uso debido o indebido que se haga sobre la información almacenada.
5. Cuando las UAA o funcionarios hagan uso o recopilen información de datos personales de miembros de la comunidad universitaria y requieran ser almacenadas en dispositivos removibles, deben cumplir con la política institucional del tratamiento de datos personales.
6. Las UAA o dependencias pueden restringir que medios de almacenamiento removibles se conecten a los equipos de cómputo que sean de su propiedad o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción, con el fin de evitar fuga de información a través de medios removibles.
7. Los medios de almacenamiento removibles que se conecten a la red de datos institucional están sujetos a monitoreo por parte de la División de Servicios de Información.
8. Todos los retiros de medios de almacenamiento fuera de las instalaciones de la UAA o dependencias, como discos duros externos, se deben realizar con la autorización del propietario del proceso misional, estratégico, mejora continua o de apoyo, definidos de acuerdo al mapa de procesos de la Universidad, a través del formato orden de salida de elementos.
9. Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros, Cintas, etc, que contengan información de carácter crítico para la UAA, la dependencia o para la misma Universidad, con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.
10. Los funcionarios responsables de custodiar los dispositivos que usan o almacenan las copias de seguridad deben controlar cualquier operación realizada sobre los dispositivos: mantenimiento, reparación, sustitución, etc. En los traslados de los dispositivos de almacenamiento a instalaciones externas a las de la Universidad, asegurar que se cumple la cadena de custodia de los mismos, para evitar fugas de información

8.5.2 POLÍTICA DE BORRADO SEGURO

1. Se deben aplicar mecanismos de destrucción y borrado de información o de sus soportes de almacenamiento cuando estos lleguen al fin de su vida útil o cuando la información ya no será más utilizada o esté obsoleta, evitando que queden al alcance de terceros.
2. Los medios de almacenamiento que contengan información de las Unidades Académico Administrativas o dependencias y que se les desea dar de baja, se sugiere que dichos medios se les apliquen técnicas de destrucción o borrado físico de manera tal que no puedan ser reutilizados para recuperar la información que en algún momento fue almacenada en ellos y que muy seguramente podría ser usada con fines indebidos; en caso tal de no poderse

perforar se les aplicar técnicas de destrucción o borrado seguro que garanticen la no recuperación de la información.

3. Todos los medios de almacenamiento que contengan información de las Unidades Académico Administrativas o dependencias, y que sean dados en donación o sean reutilizados, se les debe aplicar técnicas de destrucción o borrado lógico garantizando que la información no sea recuperable.
4. Al seleccionar o aplicar una herramienta de borrado seguro (destrucción física o lógica), elegir aquella que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo y cómo ha sido realizado.
5. En el caso de que la destrucción lógica no se realice correctamente por fallo del dispositivo, este hecho debe documentarse claramente y utilizar métodos de destrucción física de dicho soporte.
6. A los dispositivos que se les apliquen técnicas de destrucción física se debe asegurar que dichas técnicas se realicen de forma respetuosa con el medio ambiente.

8.5.3 POLÍTICA PARA LA TRASFERENCIA DE MEDIOS FÍSICOS

1. El transporte de los medios físicos que contengan información confidencial o sensible para la Universidad o para cualquiera de sus dependencias, se debe hacer mediante un medio de transporte confiable y seguro, tomando las medidas y precauciones necesarias para garantizar que los medios de almacenamiento sean transportados adecuadamente, de esta forma evitar una afectación a la integridad y disponibilidad de los mismos.
2. Se debe llevar un registro o cadena de custodia de los medios de almacenamiento físico que son transportados.
3. Las UAAs o dependencias de la Universidad deben garantizar que los medios que contienen información confidencial estén protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte.

8.5.4 POLÍTICA SOBRE ALMACENAMIENTO

1. No se permite el uso de carpetas compartidas desde equipos de escritorio. En caso tal de que un funcionario haga uso de este mecanismo se hará responsable por la pérdida o infiltración de la información o ataque informático que se pueda producir.
2. La Universidad ofrece recursos de almacenamiento de la información de forma centralizada utilizando productos comerciales en la nube y con las limitaciones definidas por el tipo de licenciamiento contratado por la Universidad.
3. Los funcionarios que utilicen la infraestructura de almacenamiento de información en la nube deben tener en cuenta las restricciones que establece el índice de información clasificada o reservada al compartir información.

4. Las UAA y sus funcionarios evitarán la divulgación no autorizada, la modificación, eliminación o destrucción de la información almacenada en los medios de almacenamiento dispuestos para tal fin.
5. Los funcionarios almacenarán la información electrónica de carácter institucional, en el lugar establecido por la Universidad, de conformidad con la Tablas de Retención Documental y acatando los lineamientos de la Dirección de Certificación y Gestión documental para la gestión de expedientes electrónicos.
6. Los funcionarios que tengan acceso a almacenar información en servidores, será responsabilidad del administrador controlar los permisos y accesos de acuerdo al criterio de lectura, escritura y modificación o de control total, según el rol del funcionario.
7. Se prohíbe el uso carpetas para el almacenamiento de archivos personales, música, videos, imágenes y cualquier otro tipo de archivo no relacionados con el cumplimiento de la función.
8. Cada funcionario es responsable directo de la generación de los backups o copias de respaldo de la información a su cargo.
9. Las UAA suministrará los recursos de almacenamiento que considere pertinente para la gestión y almacenamiento de la información por parte de los funcionarios.
10. La realización de las copias de respaldo de los servicios considerados de misión crítica que están bajo custodia y administración de la DSI serán almacenadas en un lugar seguro e interno a la Universidad, pero externo a DSI. La Ubicación de las copias de respaldo es de conocimiento único del jefe de la DSI y del líder funcional responsable de custodiar las copias de seguridad.
11. Las UAA que requieran uso de recursos informáticos para propósitos de hosting institucional deben emitir solicitud a la DSI quien evaluará y emitirá las condiciones de seguridad a seguir por parte de la UAA.

8.5.5 POLÍTICA PARA EL PRÉSTAMO DE RECURSOS INFORMÁTICOS

1. La UAA que tienen el servicio de préstamo de recursos tecnológicos, como es el caso de salas de cómputo, deben tener un lugar visible las directrices del uso debido e indebido por parte de los usuarios.
2. Los miembros de la comunidad (docentes, estudiantes, empleados, externos) deben utilizar los recursos tecnológicos de la UAA o de la Universidad (salas de cómputo, laboratorios, entre otros), como herramientas de apoyo para las labores académicas o de investigación, sin vulnerar las políticas establecidas por la Universidad o por las leyes vigentes del país.
3. Si los profesores, administrativos, estudiantes y terceros necesitan instalar, hacer uso o compartir software (libre o propio) en los recursos proporcionados por la UAA en modalidad de préstamo, deben solicitar la autorización, verificación y registro en la de la UAA que facilita la prestación del servicio.
4. Los miembros de la comunidad universitaria o terceros no deben mover o reubicar los equipos de cómputo pertenecientes a la DSI, instalar o desinstalar dispositivos, ni retirar marcas, logotipos ni hologramas de los mismos sin la autorización de la DSI.

5. Los miembros de la comunidad que hagan uso de los equipos institucionales en condición de préstamo no deberán almacenar información en estos dispositivos y deberán borrar aquellos que copien en estos al terminar su uso
6. Los recursos informáticos prestados a los usuarios no pueden ser retirados de las instalaciones de la universidad, salvo previa autorización de la UAA y del funcionario responsable en el inventario institucional.
7. Los usuarios que desean hacer uso de los servicios informáticos ofrecidos en el edificio CENTIC, deben acoger los requisitos y recomendaciones estipuladas en el catálogo de servicios informáticos de la DSI e incluso revisar las normatividades de uso del CENTIC.
8. Los miembros de la comunidad o terceros no deben abrir o destapar los equipos de cómputo de la DSI. Solo el personal autorizado de la DSI o de la División de Mantenimiento Tecnológico están autorizado para realizar esta labor.

8.5.6 POLÍTICA USO DE SISTEMAS DE VIDEOVIGILANCIAS

1. Con el fin de implementar estrategias tecnológicas que apoyen las estrategias de seguridad en la institución, la Universidad podrá hacer uso de sistemas de videovigilancia en distintos puntos geográficos del campus universitario, los cuales serán gestionados y avalados por la dirección de la División de Planta Física y cuyo objetivo será siempre velar por la seguridad.
2. Las imágenes, videos o audios grabados por medio de los sistemas de videovigilancia serán usados única y exclusivamente para el fin por el cual fueron capturadas y su custodia y tratamiento cumplirán con los requisitos establecidos en la legislación colombiana en materia de protección de datos de Carácter Personal recogidos en la Ley 1581 de 2012. Para lo expuesto, la Superintendencia de Industria y Comercio publicó la "Guía para la protección de datos personales en sistemas de videovigilancia", para brindar orientación a todas las personas y empresas que utilicen o deseen utilizar dichos dispositivos.
3. Las cámaras de seguridad como todos los dispositivos tecnológicos deben ser monitoreados y salvaguardados de acciones que conlleven a su deterioro o alteren su buen funcionamiento. Para este caso, cualquier acción que entorpezca la seguridad que pretende ofrecer las cámaras será sancionada con la normativa contenida en el Artículo 269B de la ley 1273 de 2009.
4. Los lugares que se encuentran monitoreados por sistemas de videovigilancia deben disponer de un distintivo informativo, ubicado en lugar suficientemente visible como en las zonas de ingreso o al interior de estos espacios; de manera tal que los miembros de la comunidad conozcan de la existencia de estos sistemas y las zonas videovigiladas.
5. El distintivo informativo o aviso de privacidad deben contener, como mínimo, la siguiente información: (i) datos de contacto del responsable del tratamiento; (ii) finalidades del tratamiento; (iii) derechos de los titulares de los datos personales; y (iv) la información sobre cómo acceder a la política de privacidad del responsable del tratamiento.

6. Solo las personas autorizadas pueden tener acceso a la información capturada por los sistemas de videovigilancia y dicho ingreso se mantendrá protegido por llave y/o contraseña de acceso la cual debe ser cambiada de forma periódica.
7. La División de Planta Física definirá el tiempo máximo de custodia de las grabaciones, sin embargo, dichas grabaciones se podrán mantener después del tiempo definido siempre y cuando sean objeto de investigación judicial por un robo o incidente.

8.5.7 POLÍTICA SOBRE LOS SERVICIOS DE COLABORACIÓN.

1. Las UAA solicitantes del servicio de transmisión directo o del servicio de telefonía IP se acogerán a los requisitos y recomendaciones registradas en el catálogo de servicios informáticos de la DSI.
2. La DSI es la única dependencia de la Universidad autorizada para instalar, trasladar, configurar, modificar o retirar teléfonos IP; o para ajustar o modificar las configuraciones de las salas de transmisión en directo que están bajo su custodia.
3. Las transmisiones en directo que utilicen los canales de comunicación institucional o sus redes sociales cuentan con el apoyo técnico de la DSI, pero la UAA solicitante es la responsable del contenido transmitido y divulgado por los participantes y organizadores del evento transmitido.
4. Las UAA que instalen salas de videoconferencia, deberán usar dispositivos que cumplan con las recomendaciones técnicas estipuladas por la DSI y con su aprobación para conectar los dispositivos a la red de datos Institucional
5. La DSI presta el servicio de salas de videoconferencia con un número de salas limitadas, por ende, su uso debe ser solicitado y programado con anterioridad.

8.5.7.1 Responsabilidades de los usuarios y aliados

1. El teléfono IP, quedará bajo la responsabilidad del funcionario a quien le fue asignado para sus actividades laborales.
2. Todos los funcionarios que requieran para el cumplimiento de sus funciones un servicio de telefonía deben de tener asignado un teléfono IP o un softphone (software en el computador), asignado por la Universidad.
3. Toda persona que haga uso de los teléfonos IP o salas de videoconferencia de la Universidad, utilizará estos solo en virtud de los acuerdos establecidos por los términos de licencia y será responsable por el correcto uso de éste.
4. Los teléfonos IP quedan asociados y bajo la custodia de la UAA, dependencia o área, lo que indica que éstos no pueden ser trasladados a otra UAA sin previa autorización de la DSI. Cada UAA debe hacer sus solicitudes de manera independiente.

8.5.7.2 Restricciones

1. Los teléfonos IP son los únicos que pueden ser usados dentro de la Institución, ningún otro dispositivo podrá instalarse.
2. Ningún empleado administrativo, docente o contratista está autorizado para retirar, trasladar o modificar estos equipos sin previo consentimiento por parte de la DSI

8.6 POLÍTICA DE USO DE CORREO ELECTRÓNICO

8.6.1 Generalidades

Este apartado tiene por objetivo regular el uso del correo electrónico institucional en la Universidad Industrial de Santander. Los lineamientos aquí consignados deben ser acatados por la comunidad Universitaria, integrantes de los grupos de interés internos – personal docente de planta, docente de cátedra, administrativo (sea cual fuere su forma de vinculación) y estudiantil – así como por cualquier persona integrante de algún grupo de interés externo a la que la Universidad le haya asignado - jubilado - o le asigne - contratista - un correo electrónico institucional:

1. La Universidad Industrial de Santander establece que el correo electrónico es un activo de información que se coloca a disposición de personas usuarias como una herramienta de colaboración para apoyar las actividades misionales.
2. La Universidad, por medio de la presente política, regula el uso del correo electrónico y exige a las personas usuarias su uso correcto, de conformidad con las políticas vigentes.
3. Es responsabilidad de las personas usuarias hacer lectura de este documento y acatar los lineamientos establecidos.
4. La información contenida en los buzones de correo de las **cuentas funcionales institucionales** es propiedad de la Universidad y, por lo tanto, no está permitido reenviarla a otros correos sin autorización expresa de las autoridades universitarias.
5. El servicio de correo electrónico no debe ser utilizado como repositorio para almacenamiento o respaldo de información o archivos, para ello tener presente que:
    a. La información contenida en las cuentas **personales institucionales** debe ser gestionada, de manera adecuada por cada persona usuaria, acogiendo los lineamientos de capacidad de almacenamiento institucional y realizando copias de respaldo de la información que sea pertinente.
    b. La información contenida en las cuentas **funcionales institucionales** es de propiedad de la Universidad y debe conservarse. Para evitar el llenado del buzón, esa información se guardará periódicamente en dispositivos de almacenamiento externo, de propiedad y control institucional, o en el servicio de almacenamiento en la nube que tenga contratada la universidad, y posteriormente proceder a su eliminación en el buzón de la cuenta.

6. Las credenciales de acceso para el uso correo electrónico institucional son de carácter individual; por consiguiente, ninguna persona usuaria debe utilizar una cuenta de correo que no sea la asignada por la Universidad.
7. La Universidad se reserva el derecho de aceptar o rechazar conexiones de correo electrónico desde cualquier dirección de correo electrónico o servidor externo.
8. Quien emita un correo electrónico debe identificarse (nombre, apellido, unidad interna a la que pertenece y cargo) a través de la firma, cuyo formato ha sido establecido previamente por la Universidad.
9. Es responsabilidad de quienes dirigen las diferentes UAA controlar las cuentas de correo funcionales de su unidad, asignando o reasignándolas a personas que laboren en la dependencia. Además, deberá entregarlas a la persona superior jerárquica inmediata cuando finalice la gestión de su cargo.
10. El servicio de correo electrónico de la Universidad se presta a través de contrato con un proveedor reconocido en el mercado para este tipo de servicio.
11. La División de Servicios de Información mantendrá actualizado el directorio institucional con las cuentas de correo activas.
12. Una vez asignada la cuenta de correo electrónico institucional, la persona a quien se le asigne o se le mantenga la cuenta – caso de personas pensionadas – deberá hacer uso correcto, de conformidad con las políticas vigentes.
13. Por seguridad, las personas usuarias externas que requieran tener o mantener una cuenta de correo con el dominio @uis.edu.co o con el dominio @correo.uis.edu.co no tendrán acceso a las listas de correos institucionales.
14. Toda persona externa que haga mal uso de la cuenta de correo electrónico institucional, que ponga en riesgo la seguridad de la información o que motive el bloqueo de las cuentas de correo institucionales perderá el beneficio de utilizar una cuenta de correo @uis.edu.co o @correo.uis.edu.co.

8.6.2 Límites en el número de mensajes enviados por correo

Se deben respetar estrictamente los límites en cantidad de mensajes que los usuarios puede enviar en un periodo de tiempo dado, según lo contratado por la universidad para el servicio de correo y definidos por el proveedor o plataforma contratada.

Nota: Los usuarios que necesiten enviar correos electrónicos a granel (boletines informativos, convocatorias masivas, difusión masiva de programas o eventos entre otros) deben, con la asesoría y aprobación de la DSI, utilizar proveedores de envío masivo de correo que se especialicen en este tipo de servicios.

8.6.3 Cuentas de correo funcional institucional

1. Cada unidad deberá contar al menos con dos cuentas de correo funcionales institucionales:

   a. Para la unidad: abreviacionnombreUAA@uis.edu.co o siglaUAA@uis.edu.co. Ejemplo: divfinan@uis.edu.co, dsi@uis.edu.co.
   b. Para el jefe o director: cargo.abreviaciónnombreUAA@uis.edu.co o cargo.siglaUAA@uis.edu.co. Ejemplo: jefe.inventarios@uis.edu.co, jefe.dsi@uis.edu.co.
2. Los nombres de las cuentas de correo funcionales institucionales existentes y su contenido, deberán mantenerse con el fin de conservar su recordación y la trazabilidad de la información allí contenida, la cual es propiedad de la Universidad.
3. Toda UAA, grupo o centro de investigación, curso de extensión o cualquier tipo de evento de carácter institucional deberá utilizar la cuenta de correo funcional institucional que se le asigne, en caso de requerir el correo como medio de difusión. Para estos casos, la Universidad no autoriza el uso de cuentas de correo que no correspondan al dominio institucional.
4. Toda cuenta de correo electrónico funcional institucional no tendrá el carácter de correspondencia privada y, por lo tanto, los correos electrónicos recibidos podrán ser intervenidos por la Universidad cuando lo estime conveniente.

8.6.4 Cuentas de correo personal institucional

1. La Universidad podrá asignar una cuenta de correo institucional en el dominio @uis.edu.co únicamente a personal docente y administrativo de planta. A personal estudiantil activo y a personal docente cátedra se podrá asignar en el dominio @correo.uis.edu.co. Las personas vinculadas por OPS utilizarán cuentas funcionales institucionales si la persona responsable de la UAA respectiva lo considera conveniente.
2. Las personas con el rol ya sea de estudiante, contratista o docente catedra que tengan asignada previamente una cuenta de correo institucional en el dominio @correo.uis.edu.co y que posteriormente adquieran un vínculo contractual con la universidad, seguirán usando la misma cuenta de correo en el dominio @correo.uis.edu.co para el desarrollo de las actividades institucionales.
3. Toda cuenta de correo electrónico personal institucional tendrá carácter de correspondencia privada, siendo su uso exclusivamente con fines misionales. Por ende, aunque el contenido es considerado privado, su uso debe ser solo institucional.
4. La Universidad desactivará las cuentas de correo institucional personal asignadas a los usuarios que se desvinculen de la institución, por motivos diferentes a su jubilación. En caso de cualquier comunicación relacionada con su proceso de desvinculación se utilizará un correo personal externo del exfuncionario.
5. La Universidad mantendrá activas las cuentas de correo personal institucional de sus exfuncionarios jubilados, quienes entrarán a formar parte de los grupos de interés externos y tendrán su propia lista de correos, diferente a las listas de correos institucionales.
6. Por seguridad, las personas usuarias externas que requieran tener o mantener una cuenta de correo con el dominio @uis.edu.co o con el dominio @correo.uis.edu.co no tendrán acceso a las listas de correos institucionales.

8.6.5 Responsabilidades de los usuarios

A continuación, se citan las responsabilidades de los usuarios del correo electrónico institucional:

1. Conocer y cumplir las políticas definidas en este documento.
2. Usar el correo electrónico institucional asignado únicamente para fines misionales, garantizando la no afectación al clima organizacional, ni al buen nombre de otras personas, instituciones o de la Universidad.
3. Usar la cuenta de correo funcional institucional que se le asigne solo para fines estrictamente relacionados con sus funciones y responsabilidades de tipo misional. En caso de desvinculación de la Universidad, cambio de funciones o cambio de UAA, deberá entregar a su jefe inmediato la cuenta funcional institucional que le fue asignada, preservando íntegramente la información allí contenida.
4. Controlar las cuentas de correo funcionales de la unidad, cuando es responsable de la unidad, asignando o reasignándolas a quienes considere necesario. Además, hacer entrega de éstas a la persona superior inmediata cuando realice la entrega del cargo.
5. Responder por todas las actividades realizadas con las cuentas de correo institucional que le hayan sido asignadas.
6. Notificar a la DSI cualquier situación que considere sospechosa y que podría comprometer la seguridad de su cuenta institucional, con el fin de recibir las indicaciones pertinentes.
7. Aplicar buenas prácticas de seguridad para la protección de la cuenta de correo institucional asignada, tales como, el cambio periódico de la contraseña de acceso, uso de contraseñas seguras, respaldo de la información y buen uso de la información que se envía y se recibe por este medio.
8. Aplicar las buenas prácticas de seguridad al momento de abrir correos recibidos, especialmente si se sospecha que el correo proviene de dominios desconocidos que pueden resultar maliciosos, o con contenidos sospechosos, tales como enlaces o anexos que puedan comprometer la seguridad informática de la cuenta.
9. La contraseña del correo institucional es secreta, personal e intransferible.
10. Será responsabilidad exclusiva de cada usuario realizar y mantener las copias de respaldo de la información contenida en su buzón de correo y carpetas asociadas.
11. La información consignada en las cuentas de correo institucional, relacionada con la expresión de ideas, preferencias, posiciones políticas, religiosas o de otra índole, es responsabilidad exclusiva del titular de la cuenta, por lo que este contenido no refleja ni compromete las preferencias, ideas o posiciones institucionales de la Universidad.
12. Gestionar la capacidad asignada de almacenamiento en su buzón de correo, respaldando en otro medio de almacenamiento o eliminando regularmente los documentos.

8.6.6 Uso indebido del correo electrónico

Las siguientes actividades o actuaciones se consideran como uso indebido del correo electrónico institucional:

1. Facilitar su cuenta de correo electrónico para uso de terceros.
2. Distribuir en forma masiva mensajes con contenidos inapropiados o que no correspondan a fines misionales de la Universidad. En caso de requerirse el envío de forma masiva de correos con contenido institucional, la UAA respectiva deberá utilizar una herramienta especializada en envío de correos masivos, autorizada por la DSI.
3. Enviar o reenviar a través del correo institucional cualquier tipo de mensajes de índole político, religioso, publicitario o cualquier material no relacionado con las labores misionales de la Universidad.
4. Redirigir la cuenta de correo institucional (personal o funcional) a cualquier otra cuenta, que pertenezca o no al dominio institucional de la Universidad.
5. Vincular la cuenta de correo institucional (personal o funcional) con perfiles de redes sociales personales.
6. Enviar o reenviar a través del correo electrónico institucional, mensajes contrarios a las disposiciones del orden público, la moral, las buenas costumbres, las buenas prácticas aplicables al uso de Internet y el respeto de los derechos fundamentales de las personas.
7. Enviar contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos), tales como apología del terrorismo, programas no licenciados, pornografía, amenazas, estafas, virus o código informático hostil en general.
8. Enviar mensajes que comprometan la reputación u honra de la institución o la de cualquiera de sus miembros.
9. Enviar un número alto de mensajes en un corto periodo de tiempo, que puedan dificultar o paralizar el servicio de correo electrónico o saturar la red de datos institucional. Es decir, contravenir lo expresado en el apartado “Límites en el número de mensajes enviados por correo” de este documento.
10. Falsificar encabezados de correos electrónicos, utilizar nombres de dominio que sean inválidos o inexistentes, u otras formas engañosas de enviar correo electrónico.
11. Suplantar la identidad de otra persona a través de la utilización de encabezados falsificados o de otra información personal, en el correo electrónico institucional.
12. Usar la cuenta de correo electrónico como repositorio de almacenamiento de información o como recurso de backup de información.
13. Utilizar la cuenta de **correo personal institucional** para configurar o gestionar redes sociales institucionales, convenios, proyectos o adquisiciones de bienes o servicios. En estos casos se deberá utilizar únicamente las **cuentas funcionales institucionales**.

8.6.7 Responsabilidades de la universidad

1. La Universidad se compromete a prestar el servicio de correo electrónico a través de empresas proveedoras de este servicio; sin embargo, debido a la posibilidad de problemas propios de las plataformas software que ofrecen estas empresas, a las contingencias de disponibilidad de Internet y otras situaciones imprevisibles y de fuerza mayor, la Universidad no puede garantizar la disponibilidad total de este servicio ni aceptar responsabilidades derivadas de la no disponibilidad del mismo o de pérdidas de datos por dicha causa.
2. La Universidad no se hace responsable por el manejo que la persona usuaria haga de las cuentas de correo institucional (personal o funcional) que le hayan sido asignadas.
3. La responsabilidad de la realización y el mantenimiento de copias de respaldo de la información que las personas usuarias tengan en sus buzones y carpetas de correo institucional (personal o funcional) no le compete a la Universidad sino a cada persona usuaria.
4. En caso de que una persona usuaria borre o elimine algún correo o carpeta de su cuenta de correo institucional (personal o funcional), la universidad no garantiza su reposición

8.6.8 Manejo de casos excepcionales

1. Las cuentas de correo tipo funcional institucional podrán ser intervenidas por la Universidad cuando lo considere necesario.
2. La Universidad podrá acceder a la cuenta de correo personal institucional asignada a un funcionario, en caso de requerirse.
3. La Universidad mantendrá las cuentas de correo personal institucional de los funcionarios desvinculados, durante un período máximo de tres (3) meses, con excepción del personal pensionado en vida, mientras la persona conserve el beneficio del uso del correo institucional. Vencido el plazo antes señalado, la Universidad eliminará las cuentas, con lo cual se elimina también toda información del buzón, carpetas, almacenamiento y todas las aplicaciones del proveedor de correo asociadas a la cuenta.
4. La Universidad podrá acceder a las cuentas de correo personal institucional en caso de incapacidad de la persona funcionaria por enfermedad temporal o definitiva.
5. Las cuentas de correo personal institucional asignadas a personas funcionarias vinculadas a la universidad que fallezcan durante el desempeño de sus funciones serán inhabilitadas y el contenido de sus carpetas y del almacenamiento en la nube asociado a la cuenta podrá ser mantenido durante un periodo máximo de tres (3) meses. Vencido este plazo, la universidad eliminará estas cuentas, con lo cual se eliminará también toda información del buzón, carpetas, almacenamiento y todas las aplicaciones del proveedor de correo asociadas a la cuenta.
6. Si por algún motivo la Universidad se ve obligada a suspender el servicio de correo electrónico que presta a través de un tercero, informará a sus usuarios y no tendrá responsabilidad alguna por la información contenida en los buzones, carpetas, almacenamiento y todas las aplicaciones del proveedor de correo asociadas a la cuenta.

8.6.9 Cuentas de correo en el dominio @uis.edu.co

1. El dominio @uis.edu.co es el dominio de correo electrónico institucional oficial de los miembros de la comunidad universitaria de la Universidad Industrial de Santander.
2. La Universidad podrá asignar cuentas de correo funcional institucional en el dominio @uis.edu.co a cada una de las UAA y a los cargos académico-administrativos de todo nivel existentes en la planta de personal de la Universidad. Estas cuentas serán utilizadas por las personas funcionarias que ocupen estos cargos.
3. Las personas responsables de UAA, en el periodo de su jefatura o dirección, deberán conocer las cuentas de correos funcionales adscritas a la UAA y a quienes están asignadas.
4. Las personas responsables de las UAA, en caso de requerirse para funciones misionales, podrán solicitar a la DSI la asignación de una única cuenta de correo electrónico funcional institucional en el dominio @uis.edu.co para el personal que no es planta.
5. La División de Gestión del Talento Humano deberá informar a la DSI la desvinculación de personas funcionarias, con el fin de realizar el proceso de eliminación de las cuentas de correo personal institucional que pudieran tener o eliminar la cuenta de correo de las listas institucionales y asignarla a la lista de correo que corresponda (jubilados u otras que se tengan).
6. Las personas responsables de las UAA deberán informar a la DSI (dsi@uis.edu.co) la desvinculación de las personas funcionarias o contratistas de su unidad, a quienes se les hubiera asignado cuentas funcionales institucionales, con el fin de realizar el proceso de reasignación de esas cuentas.
7. Las cuentas de correo personal institucional creadas en el dominio @uis.edu.co serán las únicas que harán parte de la lista de distribución de correo llamada institucional@uis.edu.co, con excepción de las cuentas de correo que conserven las personas que se retiren de la Institución para disfrutar de la pensión de jubilación.
8. Toda cuenta de correo que no presente actividad en un periodo de seis (6) meses consecutivos será inhabilitada y retirada de todas las listas de distribución de correo en las que esté incluida y toda la información será eliminada.

8.6.10 Cuentas de correo en el dominio @correo.uis.edu.co

1. A toda persona estudiante que ingrese a la Universidad a programas de pregrado presencial o a distancia, o a programas de posgrado se le asignará una única cuenta de correo electrónico en el dominio @correo.uis.edu.co
2. Toda persona docente de cátedra de la Universidad tendrá derecho a solicitar una única cuenta de correo en este dominio.

3. Es responsabilidad exclusiva de las personas usuarias de correo en este dominio, realizar y mantener copias de respaldo de su buzón y sus carpetas, al igual que de la seguridad de su contraseña y del buen uso de la información que se envía y se recibe por este medio.
4. La Universidad no se hace responsable por el contenido de textos, imágenes, sonidos o videos que la persona usuaria envíe o reciba usando esta cuenta de correo electrónico.
5. La Universidad no se hace responsable de las pérdidas de información que se le puedan presentar a las personas usuarias de este servicio de correo electrónico.
6. La cuenta asignada en este dominio a las personas estudiantes será la utilizada oficialmente por la Universidad para el envío de información institucional.
7. Cuando una persona estudiante pierde su condición de ser activo su cuenta de correo se deshabilita y su información podrá ser eliminada.

8.6.11 Listas de distribución de correo.

8.6.11.1 institucional@uis.edu.co

1. La lista de distribución de correo llamada "institucional@uis.edu.co" es de tipo unidireccional para el envío de información misional por parte de la dirección de la universidad.
2. Cada UAA tendrá una cuenta **funcional** institucional autorizada para el envío de información a la lista de distribución llamada **institucional@uis.edu.co**
3. A la lista **institucional@uis.edu.co** pertenecerán las cuentas de correo **personal institucional** creadas en el dominio @uis.edu.co para personas funcionarias activas, ya que en estas cuentas se recibirá información de carácter institucional proveniente de la dirección de la Universidad. Por razones de seguridad las cuentas de correo electrónico de este dominio pertenecientes a personas pensionadas no pertenecerán a esta lista.
4. Las personas usuarias pertenecientes a esta lista sólo podrán recibir los mensajes sin la opción de responder a esta lista.
5. En la lista institucional@uis.edu.co no se incluirán cuentas de correo diferentes al dominio institucional @uis.edu.co.
6. Esta lista no incluye estudiantes ni exfuncionarios que no estén vinculados en la planta de personal de la Universidad.

8.6.11.2 profesores@uis.edu.co

1. La lista de distribución de correo llamada "profesores@uis.edu.co" está conformada por las cuentas de correo **personal** institucional de los **profesores de planta** de la Universidad en el dominio institucional @uis.edu.co.
2. En la lista profesores@uis.edu.co no se incluirán cuentas de correo diferentes al dominio institucional @uis.edu.co. Por razones de seguridad las cuentas de correo electrónico de este dominio pertenecientes a personas jubiladas no pertenecerán a esta lista.
3. Esta lista no incluye cuentas de correo de personal con roles como estudiantes, contratistas, docente catedra, funcionarios administrativos y tampoco exfuncionarios jubilados.

8.6.11.3 comunidad-universitaria@uis.edu.co

1. A esta lista podrán pertenecer las cuentas de correo personal institucional en el dominio oficial @uis.edu.co de los funcionarios de planta de la Universidad que así lo deseen, previa autorización escrita del jefe inmediato. Por razones de seguridad las cuentas de correo electrónico de este dominio pertenecientes a personas jubiladas no pertenecerán a esta lista.
2. La División de Gestión del Talento Humano deberá informar a la DSI (dsi@uis.edu.co) la desvinculación de funcionarios, con el fin de retirar sus cuentas de correo de esta lista.
3. La exclusión de un correo de esta lista procederá por solicitud escrita dirigida a la DSI (dsi@uis.edu.co) por parte de la persona funcionaria responsable de la cuenta de correo institucional.
4. En ningún caso se incluirán en la lista comunidad-universitaria@uis.edu.co cuentas de correo diferentes a las pertenecientes al dominio oficial institucional @uis.edu.co.
5. Esta lista no incluye cuentas de correo de personal con roles como estudiantes, contratistas, jubilados o docente catedra.
6. A esta lista podrán pertenecer las cuentas de correo funcional institucional de las asociaciones del personal de planta legalmente constituidas y reconocidas por la Universidad.

8.6.11.4 Grupos de distribución de correo

1. Cuando una UAA requiera la creación de grupos de distribución de correo, la DSI, previa autorización de la persona responsable de la UAA solicitante podrá capacitar al funcionario designado para esta labor, en la creación y administración de los grupos requeridos. La UAA será responsable del mantenimiento y del contenido que circule a través de estas listas.
2. En cualquier caso, se deberá tener en cuenta los límites de envío del correo

8.7 POLÍTICA DE ADMINISTRACIÓN DE LA RED INSTITUCIONAL

La Universidad Industrial de Santander cuenta con una infraestructura de red de datos LAN institucional que comprende todo el cableado, switches, fibra óptica, routers, antenas y sistemas inalámbricos que permiten realizar la conexión entre estos dispositivos, los equipos servidores y los usuarios, cuya administración debe regirse por las siguientes políticas, en cualquiera de las sedes que hacen parte de la universidad:

8.7.1 Uso aceptable del servicio

1. La red LAN institucional permite a la comunidad universitaria el acceso de manera rápida y eficiente a todos sus servicios, tales como correo electrónico, navegación web, y uso de aplicaciones informáticas de misión crítica mediante conectiva alámbrica o inalámbrica.
2. Toda modificación, ampliación o remodelación de cualquier segmento de cableado estructurado en la red LAN institucional que requieran realizar las UAA, debe contar con la supervisión y aprobación de la DSI. En caso de que alguna modificación o remodelación sea

llevada a cabo por una UAA mediante un contratista externo autorizado por la universidad, esta actividad deberá contar con la aprobación de la DSI, con anterioridad a la firma del respectivo contrato. La ejecución de las obras deberá contar con la supervisión permanente por parte de la DSI y el acta de entrega y recibo a satisfacción deberá tener el visto bueno de la DSI.

3. El usuario que se conecte a la red de datos institucional ya sea a la inalámbrica o a la LAN, es el directo responsable de proteger y velar por la seguridad de la información que exponga a través de la misma.
4. La adquisición de equipos de red (switches, enrutadores, Access point, entre otros) e informáticos (servidores, PCs, portátiles, tabletas, impresoras, cámaras de video, teléfonos IP, entre otros) que deban adquirir las UAA para conexión a la red LAN institucional, debe contar con el concepto técnico de la DSI.
5. La conexión de cualquier nuevo dispositivo a la red LAN institucional, incluyendo equipos servidores, computadores, cámaras, teléfonos IP, equipos inalámbricos, entre otros, deberá contar con la supervisión y aprobación de la DSI
6. Es responsabilidad de las UAA instalar y mantener actualizadas las licencias de software de seguridad informática (anti-virus, anti-malware, firewalls, entre otros), releases y services packs en todos los equipos que necesiten conectar a la red LAN Institucional, para garantizar su plena operatividad y conectividad.
7. Las UAA que requieran conectar sus equipos servidores a la red LAN institucional, deben disponer de personal idóneo para su respectiva operación y administración técnica. En caso de presentarse cualquier incidente de seguridad informática con estos equipos, la DSI procederá a su desconexión de la red LAN
8. Todo usuario de la red LAN institucional debe informar a la DSI (dsi@uis.edu.co), a la mayor brevedad posible, cualquier anomalía que detecte en el funcionamiento de la red, con el fin de que la DSI pueda proceder con las acciones correctivas.
9. Para mantener la integridad operacional de la red LAN institucional, la DSI bloqueará o deshabilitará cualquier equipo o dirección IP que haya sido conectado o asignada sin su aprobación.
10. La conexión remota a la red de área local se permitirá, teniendo en cuenta la política de conexiones remotas de la Universidad y debe ser realizada a través de una conexión VPN segura suministrada, autorizada, registrada y auditada por la División de Servicios de Información.
11. El uso de la red inalámbrica será exclusivo para usuarios miembros de la comunidad universitaria, si alguna persona externa a la Universidad necesita acceso a la red inalámbrica institucional, lo hará accediendo a la red "INVITADO" de acuerdo a las pautas emitidas por la DSI.
12. Los profesores, administrativos y terceros que deseen que los equipos de cómputo personales accedan a la red de datos de la institución deben cumplir con todos los requisitos o controles para autenticarse en ésta y únicamente podrán realizar las tareas para el desarrollo de las funciones institucionales autorizadas.

8.7.2 Responsabilidades de la División de Servicios de Información

1. La planeación, diseño, actualización, mantenimiento y administración de la red LAN institucional es responsabilidad exclusiva de la División de Servicios de Información (DSI) de la universidad.
2. La administración y asignación de las direcciones IP públicas y privadas necesarias para la conectividad de computadores y demás dispositivos a la red LAN institucional y a internet es responsabilidad exclusiva de la DSI.
3. La DSI establecerá un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información
4. Suministrar a la UAA o a los funcionarios los lineamientos y criterios de aceptación ya sea para la instalación, modificación, ampliación o remodelación de cualquier segmento o subred de la red LAN institucional que requieran realizar las UAA
5. Emitir concepto técnico para la adquisición de equipos de red e informáticos que deban adquirir las UAA para conexión a la red LAN institucional
6. Supervisar los trabajos realizados sobre la infraestructura de red y emitir visto bueno y acta de entrega de los trabajos finalizados que cumplan con los lineamientos técnicos dados por la DSI.
7. La DSI suministrará una herramienta para realizar conexiones remotas a la red de área local de la Universidad de manera segura para los profesores y administrativos que por su labor así lo requieran, la cual debe ser aprobada, registrada y auditada.
8. La División de Servicios de Información debe asegurar que las redes inalámbricas cuenten con mecanismos de autenticación que evite los accesos no autorizados.
9. Para la protección de la red LAN y sus servicios, la DSI verificará continuamente las condiciones de seguridad de información de estos activos, y en la medida de lo pertinente elaborará y presentará las propuestas de inversión requeridas ante la dirección de la Universidad, sobre la adquisición de equipos y software necesarios para el control y mitigación de vulnerabilidades de red (firewalls, solución IPS, anti-spam, antimalware y cualquier otra herramienta de protección informática) y herramientas de monitoreo de la misma, que permitan reaccionar oportunamente ante fallas.
10. El administrador de los servicios DNS institucionales deberá revisar los dominios registrados en el DNS institucional y eliminar los que no están en funcionamiento.
11. Realizar monitoreo de los servicios y accesos aplicando correlacionamiento de log para detectar y reportar anomalías de tráfico sobre la red y servidores, y tomar las acciones correspondientes que permitan mitigar los incidentes detectados.

8.7.3 Uso indebido de la Red LAN

Se considera uso indebido del servicio de la red LAN de la universidad:

1. Utilizar la infraestructura de tecnología de información y redes de la Universidad para conseguir o trasmitir material con ánimo de lucro, excepto cuando se trate de fines institucionales. Igualmente, no se permite su utilización para realizar actividades que

impliquen acoso, difamación, calumnia o cualquier forma de actividad hostil o delictiva en contra de miembros de la comunidad universitaria o de cualquier persona o institución.
2. Ejecutar cualquier herramienta o mecanismo de monitoreo de la red sin la debida autorización de la DSI.
3. Intentar burlar los mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
4. Desconectar o manipular los elementos de red tales como switches, enrutadores, antenas, bastidores y demás elementos pertenecientes a la infraestructura de red LAN institucional sin la debida autorización por parte de la DSI.
5. Modificar la configuración de red establecida para los equipos de cómputo y de red, en cualquier dependencia de la universidad sin la debida autorización por parte de la DSI.
6. Ingresar a los centros de cableado de la red LAN institucional sin la autorización de la DSI.
7. La DSI se reserva el derecho de filtrar los contenidos que se reciban desde Internet y/o se envíen desde la red de datos institucional.
8. Transmitir información ilegal, abusiva, que ocasione responsabilidad civil o de cualquier otra índole, revele material protegido por secreto comercial o que afecte la reputación Institucional, de acuerdo con la legislación vigente y el reglamento de propiedad intelectual de la Universidad.
9. Se prohíbe el monitoreo no autorizado de datos o tráficos de la red inalámbrica y cableada de la Universidad.
10. Se prohíbe el uso de la red institucional con el fin de probar, explorar o verificar vulnerabilidades, o transgredir las medidas de seguridad informática y autenticación, o demás actos abusivos que estén estipulados por la ley.
11. Se prohíbe las transferencias de grandes volúmenes de datos, en especial si se producen de forma continua.

La DSI procederá a desconectar o desactivar de la red LAN institucional la fuente (equipo o cuenta de usuario) donde se origina cualquiera de las situaciones anteriores de uso indebido, e informará a los entes de control interno de la Universidad.

8.8 POLÍTICA DE USO DE INTERNET.

La Universidad Industrial de Santander consciente de la importancia del uso de Internet como una herramienta para el desarrollo de sus actividades misionales y de apoyo, proporciona los recursos necesarios para asegurar la disponibilidad del servicio de internet a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la Universidad, para ello establece:

8.8.1 Uso aceptable del servicio

1. El servicio de Internet institucional solo se ofrece por medio de la infraestructura hardware software de la red local institucional gestionada por la División de Servicios de Información (DSI).
2. Las UAA que contraten una conexión a internet diferente a la provista por la Universidad deberán tener en cuenta las políticas de seguridad informática establecidas institucionalmente y contarán con la autorización previa y la supervisión de la DSI para dicho contrato. En este caso, la UAA contratante será responsable de mantener las políticas de seguridad informática establecidos para la red institucional y definidos por la DSI.
3. El servicio de Internet institucional se debe emplear como una herramienta para investigación, desarrollo, consulta y comunicación de actividades relacionadas con los procesos misionales y de apoyo de la Universidad Industrial de Santander.
4. El servicio de Internet de la universidad puede ser utilizado con fines didácticos permitiéndole a los usuarios tomar cursos de capacitación por Internet en temas que enriquezcan su labor dentro de la institución.
5. Este recurso podrá ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la Universidad.
6. Al utilizar el servicio de Internet de la Universidad, se espera que el usuario (estudiante, docente, administrativo o contratista) use los servicios con respeto, cortesía y responsabilidad, en procura de no vulnerar los derechos de los demás usuarios de este servicio y realizando una gestión adecuada para la protección de la información que puede circular por medio del mismo.
7. El acceso a determinadas páginas de Internet puede ser bloqueado para usuarios individuales, grupos de usuarios o para todos los empleados, servidores o colaboradores de la Institución, dependiendo del monitoreo y análisis de navegabilidad aplicado a las mismas por parte de la División de Servicios de Información. Si el acceso a algunas páginas Web está bloqueado, el usuario puede elevar una petición escrita solicitando autorización para acceder a dichas páginas. El usuario no debe intentar eludir por su cuenta esa restricción.
8. El servicio de Internet es el medio de difusión del sitio web institucional de la Universidad y de acceso a los servicios que sobre ésta presta la Universidad.
9. El personal externo al cual la Universidad le permita el acceso a internet se acoge a los lineamientos de conectividad de la red y acepta las responsabilidades en las que incurre por ser usuario de esta y del servicio de internet.
10. Los servicios a los que un miembro de la comunidad universitaria puede acceder desde internet dependerán de su rol institucional.
11. El acceso a internet desde dispositivos móviles se hará bajo la credencial de acceso institucional asignada de forma personal a cada miembro de la comunidad, la cual tiene correspondencia con la asignada para el ingreso a determinados servicios informáticos.
12. Considerar como no confiable la información recibida a través de sitios web no verificados en vista que dicha información puede ser utilizado con fines comerciales o delictivos.

13. Todas las comunicaciones enviadas o recibidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control de la Universidad.

8.8.2 Responsabilidades de los usuarios

1. Los usuarios autorizados del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información o el funcionamiento del servicio.
2. Los usuarios son responsables de informar sobre contenidos o acceso a servicios que no le estén autorizados y/o no correspondan a sus funciones/actividades dentro de la Universidad.
3. Abstenerse de suministrar sus credenciales de acceso a internet a otros funcionarios o personal externo.
4. El usuario es responsable por todas las posibles consecuencias que surjan por el uso no autorizado o inadecuado de servicios o contenidos de Internet.
5. Cada uno de los funcionarios serán responsables de dar un uso adecuado de este recurso y en ningún momento podrá ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, entre otros.

8.8.3 Responsabilidades de la División de Servicios de Información

1. Definir los lineamientos para la contratación del(os) proveedor(es) que ofrecerán el servicio de internet a la comunidad universitaria.
2. Gestionar el servicio de internet contratado y mantener las relaciones con el (los) proveedor(es) responsable del servicio para garantizar el funcionamiento y mantenimiento adecuado y eficiente de Internet.
3. Monitorear permanentemente los canales del servicio navegación de internet, verificando el mantenimiento de la calidad del servicio hacia la comunidad universitaria.
4. Generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet, preservando el derecho fundamental a la intimidad.
5. La DSI se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación que presenten un comportamiento inusual o sospechoso, al igual que filtrar los contenidos que se reciban desde Internet y/o se envíen desde la red de la universidad.
6. Proteger el servicio de navegación sobre internet mediante cortafuegos adecuados y la implementación de requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.

7. Establecer los procedimientos e implementar controles para evitar la descarga de software no autorizado, código malicioso proveniente de Internet y el acceso a sitios catalogados como restringidos.
8. Diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
9. Emitir orientaciones a los usuarios sobre las precauciones a tener en cuenta cuando se detecten ataques mal intencionados sobre el servicio de internet.

8.8.4 Uso Indebido de Internet

Se considera uso indebido del servicio de internet de la Universidad:

1. Ingresar a páginas web cuyo contenido o autoría sea objetable o ilegal.
2. Acceder a contenidos de sitios web pornográficos, de grupos alzados en armas, de grupos terroristas o de sitios dedicados a difundir temas relacionados con violencia de cualquier tipo, al igual que promover o difundir a nombre de la universidad dichos contenidos.
3. Utilizar el canal de conexión a Internet para descargar e instalar contenido digital (música, videos, archivos ejecutables, entre otros) que infrinja derechos de autor o cualquier tipo de software no licenciado por la Universidad.
4. Participar de juegos en línea o realizar actividades de tipo comercial en línea, salvo aquellas actividades que, en atención a la necesidad del servicio por motivos de índole institucional, sean autorizados por el jefe de la UAA respectiva.
5. Hacer uso del servicio de Internet de la Universidad para participar de cualquier actividad ilegal o que atente contra el ordenamiento jurídico vigente.
6. Ingresar a internet por medio de sus credenciales de acceso desde dispositivos móviles que no son de su uso exclusivo y dejar grabadas las credenciales de acceso de forma predeterminada.
7. Acceder a páginas relacionadas con anonimizadores, actividades relacionadas con crímenes computacionales, hacking, discriminación, contenido malicioso, suplantación de identidad, spyware, adware, redes peer to peer (p2p), o páginas catalogadas como de alto riesgo dictaminado desde la herramienta de administración y monitoreo de navegabilidad.
8. Enviar y/o descargar información masiva de gran tamaño que pueda congestionar la red y que no corresponde para el desarrollo de las actividades institucionales.
9. Enviar, descargar y/o visualizar información con contenidos que atenten contra la integridad moral de las personas o instituciones.
10. Una vez finalizada la vinculación de un funcionario con la Universidad, cualquiera que haya sido su modalidad, deberá abstenerse de continuar usando las cuentas de acceso a la red, al servicio de Internet y a cualquier servicio informático institucional.
11. Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.

En caso de que la DSI detecte la realización de alguno de estos procedimientos no permitidos, procederá a informar a los entes de control interno de la Universidad.

8.9 POLÍTICA DE REDES SOCIALES

Los perfiles oficiales de la Universidad en las redes sociales son responsabilidad de la Dirección de Comunicaciones de la Universidad.

8.9.1 Uso aceptable del servicio.

1. La Dirección de Comunicaciones es la Unidad encargada de definir las directrices y procedimientos generales para el uso institucional del servicio de las redes sociales y de las plataformas autorizadas de una manera institucional.
2. La Universidad permite el uso de las redes sociales teniendo en cuenta que estos medios se constituyen en un complemento de comunicación, divulgación y socialización con la comunidad sobre las actividades relacionadas con la Unidad Académico-Administrativa, sin embargo, es necesario utilizarlos de forma correcta y moderada.
3. Las Unidades Académico Administrativas que faciliten el uso del servicio de redes sociales deben establecer el (los) funcionario(s) responsable(s) de gestionar el servicio de acuerdo a los lineamientos dados por la Dirección de Comunicaciones.
4. Los funcionarios autorizados para usar los servicios de Redes Sociales Institucionales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información de la Universidad o de algún miembro de la misma.
5. La Dirección de Comunicaciones se reserva el derecho de: a) monitorear las comunicaciones y/o información que presenten un comportamiento inusual o sospechoso, b) filtrar los contenidos; que se reciban o envíen desde las redes sociales de la Universidad.
6. Es permitido el uso de redes sociales utilizando video conferencia y streaming teniendo en cuenta los lineamientos dados por la DSI para las transmisiones vía streaming en su catálogo de servicios.
7. El funcionario que publique o divulgue a título personal, por cualquier red social, información de otro miembro de la comunidad universitaria, contratista o colaborador de la Universidad, se considerará fuera del alcance del Sistema General de Seguridad y Privacidad de la Información y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.
8. La Dirección de Comunicaciones en coordinación con la Dirección de Certificación y Gestión Documental, velará por emitir lineamientos y efectuar prácticas que permitan una adecuada gestión, archivamiento y conservación de la información divulgada por medios sociales.
9. La Universidad suministrará los recursos necesarios que permitan dar el cumplimiento de los lineamientos expuestos en la presente política.

8.9.2 Uso indebido del servicio

1. Descargar, difundir o distribuir material obsceno, degradante, terrorista, abusivo o calumniante a través del servicio de Redes Sociales.
2. Publicar información con contenidos que atenten contra la integridad moral de las personas o de la Universidad.
3. Intentar violar o aprovechar el acceso a Redes Sociales para fines ilegales.
4. Los funcionarios de la Universidad no deben crear cuentas, abrir grupos, o publicar cualquier tipo de información escrita o audiovisual a nombre de la Universidad o Unidades académicas administrativas sin la autorización respectiva de la UAA.
5. Utilizar el nombre de la Universidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la Universidad Industrial de Santander.

8.10 POLÍTICA TRATAMIENTO DE DATOS PERSONALES

La Universidad Industrial de Santander en cumplimiento de sus obligaciones como entidad pública y acatando lo emanado por la ley 1581 de 2012, propende por la protección de los datos personales de los miembros de su comunidad universitaria y demás personal externo de los cuales recibe o administra información. En correspondencia a lo expuesto, la Rectoría de la Universidad emite la Resolución n.° 1227 de agosto 22 de 2013 por la cual aprueba el Manual de Procedimientos Administrativos para el Tratamiento de Datos Personales.

Acudiendo a los principios de la Administración Pública, previstos en el artículo 209 de la Constitución Política, es responsabilidad de todo funcionario o persona particular que posea algún tipo de vínculo de cualquier índole con la Universidad conocer y aplicar el Manual de procedimiento administrativo para el tratamiento de datos personales.

Las UAA que en el desarrollo de sus funciones recopilen datos personales están en la obligación de recibir autorización y aprobación del propietario de los datos siguiendo las directrices aprobadas en el Manual institucional de procedimiento administrativo para el tratamiento de datos personales. En consecuencia, queda prohibida la recopilación de datos personales sin la autorización del titular de estos.

Los titulares de los datos personales que suministren sus datos a la Universidad podrán hacer uso de los lineamientos definidos en el Manual institucional de procedimiento administrativo para el tratamiento de datos personales, para hacer valer sus derechos en el caso que se realice un trato indebido de sus datos por parte de la Universidad.

El titular de la información tiene derecho a optar por no suministrar cualquier información sensible solicitada por la Universidad, tales como: datos sobre su origen racial o étnico, la pertenencia a

sindicatos, organizaciones sociales o de derechos humanos, convicciones políticas, religiosas o filosóficas, de la vida sexual, biométricos o datos de salud, la captura de imagen fija o en movimiento, huellas digitales, fotografías, iris, reconocimiento de voz, facial o de palma de mano, etc.

La Oficina Asesora Jurídica conceptuará a través de un documento tipo manual o guía, sobre el tratamiento de los datos personales en la Universidad, a partir de la identificación del tipo de datos, clases de datos o tipo de información que la Universidad recopile, procese o almacene en el desarrollo de sus actividades misionales y de apoyo. Ejemplo:

- ✓ Tipo de dato: profesionales, financieros, sensibles, etc.
- ✓ Clase de datos: nombres, teléfonos, cedula, direcciones, etc
- ✓ Tipo de información: fotografías, imágenes en movimiento, huellas digitales, etc.

Las UAA y propietarios de activos de información que recopilen, procesan o resguardan datos personales deben implantar los controles necesarios para custodiar y proteger los datos personales, y ejecutar los controles sobre el almacenamiento de las bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

Las UAA establecerán y divulgarán los términos, condiciones y finalidades para las cuales recopilarán la información en función de las actividades que desarrollan y establecerán sus responsabilidades con el tratamiento de los datos personales obtenidos en sus distintos canales.

Los funcionarios de la Universidad deben guardar la discreción correspondiente o la reserva absoluta con respecto a la información de la Universidad o de sus funcionarios o de terceros de la cual tengan conocimiento en el ejercicio de sus funciones.

Los funcionarios de la Universidad deben aplicar en la medida de lo posible. mecanismos que permitan verificar la identidad de todas aquellas personas a quienes se les entrega información por teléfono, por correo electrónico o certificado, entre otros.

Los propietarios de los activos de información de las diferentes UAA deben asegurar que tendrán acceso a los datos personales únicamente los funcionarios que en relación del cumplimiento de sus funciones tengan la necesidad legítima de acceder a ellos.

8.10.1 Anonimización de datos personales

La Universidad acogiendo los lineamientos del Estado Colombiano sobre el respeto de los derechos de las personas y consciente de la importancia de un adecuado tratamiento de los datos personales, definirá directrices y aplicará técnicas adecuadas y pertinentes para la anonimización de datos personales recopilados, desde los diferentes procesos institucionales, para ser publicados en datos abiertos o que conlleven a la generación, entrega o publicación de archivos para el estudio, análisis o

generación de estadísticas; con el fin de evitar la identificación o reducir las probabilidades de reidentificación de sujetos individuales en pro de garantizar la privacidad de sus datos personales.

En correspondencia a lo anterior, cada UAA responsable de la publicación o generación de la información destinada a estudio, análisis o generación de estadísticas deberá acatar los lineamientos establecidos por la Universidad con el objeto de garantizar el proceso de anonimización de datos personales.

8.11 CONTROLES DE ACCESO LÓGICO

La Universidad Industrial de Santander por medio de las UAA, propietarias de los Activos de Información considerados sensibles, y en apoyo de la División de Servicios de Información definen las pautas y procedimientos generales para controlar y monitorizar los accesos lógicos a los medios de información considerados, a su vez, de misión crítica y que estén bajo la custodia de la DSI, como son los sistemas de información, bases de datos, aplicaciones y redes, entre otros.

Las UAA propietarias de los activos que concedan acceso a usuarios, deben controlar dichos accesos solo por el tiempo que sea necesario para el desarrollo de las tareas.

Los accesos y protección a los servicios informáticos, divulgados en el catálogo de servicios de la División de Servicios de Información, está determinado por el esquema de seguridad definido por la DSI y se basa en la estructura de roles – usuarios, enmarcado a su vez en el principio de asignación del mínimo privilegio para el cumplimiento de las labores del usuario.

Las UAA que autoricen acceso a los servicios informáticos deben hacer firmar a los usuarios o miembros de la comunidad acuerdos de confidencialidad o de no divulgación sobre la información a la cual tendrán acceso.

8.11.1 POLÍTICA DE CONTROL DE ACCESO A REDES Y SERVICIOS EN RED

El control de acceso y monitoreo sobre las redes y servicios de red institucional, están a cargo de la División de Servicios de Información (DSI) y para ello la Universidad establece que:

1. La DSI velará por a) aplicar los controles para protegerla la red de datos de los accesos no autorizados, b) generar registros sobre el monitoreo y acceso a dichos servicios, c) detectar actividades anómalas respecto al acceso y uso de los servicios de red, d) informar a los responsables de los procesos sobre los hallazgos detectados.
2. La DSI suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, garantizando la segregación de

tareas y limitando la autorización de acceso solo a la información indispensable para la ejecución de las labores asignadas.

3. La DSI divulgará las directrices para solicitar el acceso a los diferentes servicios informáticos, a cargo de esta División, por medio del catálogo de servicios publicados en la página web, tales como: correo institucional, publicación de páginas web y portales UAA, préstamo de equipos y salas, red cableada e inalámbrica, diseño y mantenimiento de software entre otros ~~(ver aquí)~~
4. Solo el personal designado por la DSI, está autorizado para instalar software o hardware en los dispositivos que forman parte de la infraestructura de telecomunicaciones de la Universidad.
5. Todo trabajo que requiera acceder a los servidores o dispositivos de la red institucional, se debe realizar en las instalaciones de la Universidad. No se podrá realizar ninguna actividad de tipo remoto sin la debida autorización de la DSI.
6. La conexión remota a la red de datos institucional de la Universidad debe ser realizada a través de una conexión VPN segura suministrada por la DSI, la cual será autorizada por la UAA a la cual se desea acceder, y registrada y auditada por la DSI.
7. La DSI garantizará que las redes inalámbricas de la Universidad cuenten con métodos de autenticación y cifrado que eviten accesos no autorizados.
8. La DSI establecerá los lineamientos para ajustar los permisos de acceso a la red y servicios de red, asignados a los usuarios de los sistemas de información y comunicaciones, tomando como base los múltiples factores de riesgo existentes en la seguridad de la información.
9. En la situación de los proveedores que prestan servicios a las diferentes UAA y que requieran acceder a través de una cuenta institucional a los servicios y recursos informáticos de la Universidad en aras de cumplir a cabalidad con las obligaciones del contrato, las UAA deberán hacer la solicitud de activación e inactivación de dicho acceso ante la DSI quien analizará la justificación teniendo la facultad de aprobarla o negarla.
10. Aquellos proveedores con los cuales se contratan servicios de administración sobre Sistemas de Información y plataformas tecnológicas que se encuentren bajo la custodia de la DSI, podrán tener acceso al ambiente de producción previa autorización de la DSI y bajo un contrato firmado que refleje el objeto de la prestación del servicio e incluya una cláusula de confidencialidad.

8.11.2 POLÍTICA ADMINISTRACIÓN DE LOS ACCESOS DE LOS USUARIOS

Tal como se había enunciado previamente, la DSI es la dependencia de la Universidad encargada de garantizar el acceso a los diferentes servicios informáticos que apoyan las actividades misionales de carácter crítico de la Universidad, permitiendo que los usuarios autorizados accedan únicamente a los servicios aprobados y restringiendo el acceso a los no autorizados.

8.11.2.1 Credenciales y registros de acceso de usuarios

1. La DSI asignará un ID de usuario y contraseña de acceso a los funcionarios para que estos puedan acceder a los servicios informáticos institucionales a cargo de la DSI.

2. Para efectos institucionales el ID de usuario y la contraseña de acceso recibirán el nombre de credenciales de acceso.
3. A cada credencial de acceso se le asignarán permisos y roles de acuerdo a las funciones institucionales a realizar y al esquema de seguridad establecido por la DSI
4. La DSI velará por reducir la existencia de ID de usuarios redundantes eliminándolos de forma periódica y en caso de no poderlo hacer evitar que nunca sean asignados a otros usuarios.
5. La DSI y en corresponsabilidad con el propietario del activo de información controlarán el alta y baja de las credenciales de los usuarios que acceden a los sistemas de información y a otros servicios informáticos a cargo de la DSI.
6. Las credenciales de acceso deberán ser desactivadas/canceladas de forma inmediata cuando el usuario abandone la Universidad y para ello el propietario del activo que solicitó el acceso del usuario deberá informar a la DSI o en su defecto, en caso de existir, hacer uso del aplicativo dispuesto en su UAA para tal fin.
7. Las DSI gestionará los registros de acceso de los usuarios a los servicios informáticos institucionales a cargo de la DSI.
8. Los registros de los usuarios no serán eliminados y se mantendrán en el histórico, en vista de las particularidades de operatividad de la Universidad.

8.11.2.2 Gestión de acceso a los usuarios.

Las directrices de esta política propenden por garantizar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios de información.

8.11.2.2.1 Responsabilidades de los Usuarios.

1. El acceso a los activos de información se hará utilizando las credenciales de acceso asignadas por la DSI.
2. No participar en actividades que puedan ser utilizadas para eludir controles de seguridad de los sistemas de información o cualquier otro recurso informático de la Universidad.
3. Mantener en secreto las credenciales de acceso ya que son de uso personal e intransferible, por ende, no se debe compartir sus cuentas de usuario y contraseñas con otros funcionarios o terceras partes.
4. No permitir directa e indirectamente que otra persona utilice sus credenciales de acceso o utilizar los de otros usuarios.
5. Asumir las acciones y consecuencias que llegasen a realizarse desde la cuenta de usuario asignada y/o los privilegios otorgados.
6. Acogerse a los lineamientos establecidos sobre el manejo y buenas prácticas para el uso de las contraseñas o cuentas de acceso estipuladas en la política.
7. Reportar a la DSI sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.
8. Informar oportunamente a la DSI y a la UAA sobre cualquier inconveniente con los accesos de usuario, ya sea por exceso o falta de permisos, para acceder a la información, absteniéndose de utilizar los privilegios concedidos de forma errada.

9. No está permitido usar las credenciales de acceso en herramientas o programas utilitarios que permitan el acceso a los sistemas, bases de datos o servicios de red sin previa autorización del custodio del recurso o servicio tecnológico, evadiendo así los controles de seguridad implementados por el responsable de los mismos.

8.11.2.2.2 Responsabilidades de las UAA

1. Solicitar la creación y aprobación de las cuentas de acceso de los funcionarios que necesitan acceder a los sistemas y servicios informáticos Institucionales acogiéndose a los procedimientos definido por la DSI
2. Informar a la DSI sobre el retiro o cambio de rol de un funcionario dentro de la UAA solicitando la eliminación, desactivación o revocación de las credenciales de acceso asignadas al funcionario para cumplir con sus funciones dentro de la UAA.
3. Las UAA deben revisar, por lo menos una vez cada 12 meses, los roles en cada sistema de información asignado a los funcionarios de la UAA respectiva e informar a la DSI sobre cualquier inconsistencia.
4. Informar a la DSI cuando se detecte alguna anomalía sobre el uso indebido de las credenciales de acceso a los servicios informáticos institucionales.
5. Es responsabilidad del jefe de la UAA las acciones que pueda realizar el personal externo para el cual se le solicitaron credenciales de acceso.

8.11.2.2.3 Responsabilidades de la DSI

1. Divulgar las directrices que deben seguir las UAA para la solicitud y aprobación de la creación de las cuentas de acceso de sus funcionarios que requieren acceso a los sistemas y servicios informáticos.
2. Mantener actualizado el catálogo de servicios de la DSI y los procedimientos que indican las directrices a seguir por parte de las UAA para la administración de los usuarios que asegure la creación, modificación, bloqueo o eliminación de cuentas de usuario, sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna cuando los funcionarios se vinculan, desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.
3. Crear las credenciales de acceso de los funcionarios autorizados asegurando la asignación de los permisos respectivos para el cumplimiento de sus funciones y restringiendo los que no requiere.
4. Comunicar al funcionario, previa validación de la identificación del funcionario, las credenciales de acceso asignadas para su ingreso a los servicios institucionales utilizando un medio de comunicación seguro.
5. Revocar o cancelar los permisos de acceso asignados a los funcionarios que abandonan la Universidad o cambian de rol, previa notificación de la UAA a la cual está inscrito el funcionario o miembro de la comunidad. Cabe aclarar que las credenciales de acceso asignadas no serán eliminadas cuando el funcionario abandona la UAA en vista de la diversidad de las actividades de vinculación con la Universidad.

6. Cuando un funcionario ha cambiado de rol dentro de la Universidad, garantizar la asignación de los permisos que le permitan al funcionario acceder a los sistemas y servicios informáticos para el cumplimiento de sus funciones, previo cumplimiento del proceso de autorización por la UAA respectiva.
7. Registrar los accesos exitosos y fallidos a los sistemas de información y tecnologías considerados sensibles, con el fin de identificar y alertar posibles amenazas de accesos y cambios no autorizados.
8. Mantener registro de actividades realizadas por los usuarios de los sistemas de información o servicios de red, sobre la información o conexiones consideradas sensibles o que requieren ser auditadas.
9. Verificar periódicamente los controles de acceso de los usuarios, con el fin de revisar que éstos tengan acceso permitido únicamente a aquellos recursos de red y servicios a los recursos tecnológicos para los que fueron autorizados.
10. Realizar seguimiento y análisis a los registros de acceso de los usuarios y a sus actividades con el fin de detectar actividades anómalas.
11. Finalizar las sesiones de usuarios por vencimiento del periodo de inactividad sobre los sistemas o servicios tecnológicos institucionales.

8.11.2.3 Gestión de derechos de acceso privilegiados.

1. La DSI mantendrá los registros y realizará seguimientos a las actividades sobre los sistemas de información o servicios por parte de usuarios con permisos elevados (administrator, root, etc.), para analizarlos y de esta forma, identificar riesgos a los que se están exponiendo los sistemas de información y recursos de red, con las actividades de dichos usuarios.
2. Las UAA que aprueben acceso a usuarios con acceso privilegiado, como administradores de sistemas de información o aplicativos, deben auditar de manera ocasional las acciones de los mismos.
3. Los líderes funcionales de la DSI establecerán los lineamientos para los usuarios con acceso privilegiado a los ambientes de desarrollo, bases de datos, sistemas, servidores y áreas de procesamiento de información, entre otros.
4. Los administradores de servidores o DBA no suministrarán a los desarrolladores credenciales de acceso a los sistemas de información, a los servidores y bases de datos institucionales en el ambiente de producción.

8.11.2.4 Gestión de contraseñas para usuarios.

1. Las claves o contraseñas son de uso personal e intransferible y es responsabilidad del usuario el uso adecuado o inadecuado de las credenciales asignadas. Por ende, no está permitido prestar, divulgar o difundir la contraseña de acceso, ni la propia ni las de compañeros o jefes, a otras personas que lo soliciten.
2. Las claves de acceso no deben ser escritas en elementos que estén a la vista o permanezcan desatendidos o sin protección de acceso.
3. Las contraseñas que se suministran de forma genérica deben ser cambiadas la primera vez de inicio de sesión por parte del usuario.

4. No utilizar las claves de uso personal de trámites comerciales o financieras, para los fines de acceso a los sistemas o servicios informáticos institucionales.
5. No guardar las contraseñas de acceso a los sistemas de información o servicios informáticos institucionales en navegadores web y en particular si el equipo de cómputo a utilizar es de uso compartido.
6. Abstenerse de usar contraseñas de fácil detección como datos personales, nombres de familiares, palabras usadas frecuentemente, uso de patrones como secuencias de números o caracteres y cadenas repetidas.
7. Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que esta expire.
8. Los usuarios deben cambiar inmediatamente la contraseña si tiene la sospecha de que esta es conocida por otra persona.
9. Al asignar o reasignarse contraseñas incrementar el nivel de complejidad usando mayúsculas, minúsculas, números y por lo menos un carácter especial y de una longitud mayor a 8 caracteres.
10. La UAA que suministre contraseñas de acceso debe garantizar la seguridad del canal de comunicación utilizado para impartir la contraseña, previa validación de la identificación del usuario propietario de la cuenta de acceso.
11. Las UAA que gestionen contraseñas deben mantener un registro de las 3 últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
12. Las UAA que gestionen contraseñas deben garantizar que se almacenen en forma cifrada utilizando un algoritmo de cifrado unidireccional.
13. La DSI garantizará la transmisión segura de contraseñas sobre la red.
14. La DSI proporcionará los mecanismos necesarios para que los miembros de la comunidad universitaria que olviden, bloqueen o extravíen su contraseña, puedan restablecerla de forma segura.
15. Los mecanismos de autenticación utilizados para acceder a sistemas de información o servicios, deben obligar al usuario a cambiar la contraseña por lo mínimo cada seis meses y rechazar las contraseñas débiles.
16. Todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware (por ejemplo: appliance, impresoras, routers, switch, herramientas de seguridad, etc.) deben ser cambiadas por una personalizada siguiendo las pautas anteriores.
17. Las contraseñas de acceso a los servidores y administración de los Sistemas de Información deben ser cambiadas mínimo cada seis (6) meses.
18. La contraseña de los usuarios con acceso privilegiado y que usan cuentas de acceso genérico, deben ser cambiadas una vez el usuario haya abandonado la Universidad o cambiado de cargo.

8.11.2.5 Controles de acceso sobre el código de programas fuentes.

La DSI es la dependencia de la Universidad responsable de definir las actividades necesarias para llevar a cabo el desarrollo o mantenimiento de software y el procesamiento de datos, para las Unidades Académico Administrativas de la Universidad Industrial de Santander. En consecuencia, velará por aplicar controles que protejan el código fuente de los sistemas de información desarrollados la DSI, por consiguiente, es responsabilidad de la DSI:

1. Por medio de los líderes funcionales, generar lineamientos para restringir y auditar el acceso a los códigos fuentes de los programas y elementos asociados como (diseños, especificaciones, librerías de fuentes de programas, planes de verificación y planes de validación).
2. Establecer los procedimientos de preproducción y producción para acceso de los desarrolladores a los ambientes de desarrollo.
3. Por medio del líder funcional de desarrollo, hacer conocer dichos procedimientos a los desarrolladores a cargo.
4. Restringir, a nivel de los aplicativos, el acceso a archivos de configuración u otros recursos, a direcciones URL protegidas, a funciones protegidas, a credenciales, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados; siguiendo las pautas definidas en el esquema de seguridad definido por la DSI para los sistemas de información.
5. Asegurar que los sistemas de información construidos exijan autenticación para todos los recursos y operaciones ejecutadas con el software.
6. Establecer los controles de autenticación que eviten la visualización de contraseñas.
7. Garantizar que no se almacenen contraseñas, cadenas de conexión u otra información pública clasificada y pública restringida en texto claro y que se implementen controles de integridad de dichas contraseñas.
8. Implementar en el software controles que obliguen al usuario a cambiar la contraseña por defecto en el primer ingreso.
9. Implementar los controles necesarios para asegurar que el acceso al código fuente de los aplicativos desarrollados sea limitado. Solamente el personal del grupo de desarrollo podrá contar con acceso a esta información y hará un uso moderado de la misma.
10. Proporcionar las herramientas necesarias para realizar control de cambios sobre el código fuente de los aplicativos desarrollados, las cuales permitirán retroceder a una versión anterior del código.
11. Aprobar, supervisar y modificar los códigos fuente de los aplicativos siguiendo el procedimiento y estándares de desarrollo definidos por la DSI.
12. Los administradores de servidores y DBA verificarán y asegurarán que los desarrolladores, administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción o en su defecto asegurar que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.

13. Los líderes de desarrollo de los sistemas de información institucionales autorizan o revocan el acceso al código fuente de los sistemas de información institucionales desarrollado por la DSI.
14. La DSI, por medio de los líderes funcionales, los administradores de servidores y DBA, definirán los procedimientos y controles que asegurarán que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción, pruebas y desarrollo de los sistemas de información, redes de datos y los recursos de red a cargo de la DSI.

8.11.2.6 Revisión de los derechos de acceso de los Usuarios

Los derechos de acceso de los usuarios a los servicios informáticos y a la infraestructura de procesamiento de información de la Universidad, deberán ser revisados periódicamente por los responsables de las UAA y cada vez que se realicen cambios, en los roles del personal o grupos de trabajo que impliquen modificación en los permisos de acceso a los recursos informáticos, deben informar a la DSI.

8.11.2.7 Retiro de los derechos de acceso

1. La UAA será la encargada de informar a la Dirección de Gestión de Talento Humano y esta a su vez a la DSI, sobre el cambio de cargo, toma de licencias, vacaciones, funciones/actividades o la terminación contractual de los funcionarios o contratistas que realizan actividades con la UAA y que tengan acceso a los servicios informáticos institucionales, con el fin de que la DSI retire los derechos de acceso a los servicios y procesamiento de información.
2. El integrante de la comunidad universitaria que haya adquirido el rol de estudiante inactivo, indistintamente del nivel de estudio, perderán el acceso a los servicios informáticos.

8.11.3 POLÍTICA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN UIS

La Universidad Industrial de Santander para garantizar una gestión adecuada de la seguridad de los sistemas de información, establece que:

1. La División de Servicios de Información definirá la estructura técnica de seguridad bajo el cuales se desarrollará y accederá a los sistemas de información que apoyan la gestión de los procesos de la Universidad.
2. La UAA responsable de un sistema de información definirán los niveles de acceso de los usuarios que utilizarán el sistema, basada en las funciones institucionales desempeñadas por el funcionario.
3. Los datos de acceso de los usuarios los asignará la DSI teniendo en cuenta los lineamientos para la gestión de las credenciales de acceso.

8.11.3.1 Entorno De Navegación

Para cada sistema de información, la UAA responsable define los roles necesarios para el adecuado uso del sistema de información de acuerdo a las funciones que realice y establece los usuarios asociados a cada uno de ellos.

Para cada rol se define el menú de inicio, el cual le permite a cada usuario que hace parte de este rol, empezar la navegación por las distintas opciones que le ofrece el sistema, hasta llegar al nivel más bajo en el cual se ejecuta el proceso que soporta la actividad que desea realizar.

8.11.3.2 Entorno De Control De Datos

Para los roles definidos en cada uno de los sistemas de información se especifican las tablas a las cuales puede acceder, el tipo de transacción que puede realizar sobre estas tablas (inclusión, modificación o eliminación de registros), si tiene acceso total o parcial a la información que contiene la tabla.

Para el acceso a la información de la tabla de manera parcial, se deben establecer atributos y los valores que estos atributos deben tener para autorizar el acceso solicitado.

8.11.3.3 Auditoría

Las tablas de las bases de datos que se consideren criticas dispondrán de un historial de las transacciones realizadas sobre cada una de ellas.

El historial de las transacciones de cada tabla contiene información de los registros incluidos en la tabla, de los registros modificados y de los registros eliminados. Adicionalmente, en cada transacción se especifica: Fecha de la transacción, hora de la transacción, tipo de transacción (I/U/D), tipo y número de documento de identidad del usuario que realizó la transacción, usuario y rol asociado

8.12 POLÍTICA SEGURIDAD FÍSICA Y DEL ENTORNO

La Universidad Industrial de Santander, por medio de las UAA, evitará accesos físicos no autorizados a las instalaciones de procesamiento o resguardo de información, que generen afectaciones a la confidencialidad, integridad o disponibilidad de la información.

La UIS por medio de la División de Planta Física proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus

instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de los edificios y oficinas.

La División de Planta Física en conjunto con la División de Servicios de Información debe asegurar que las labores de mantenimiento de los activos de comunicación de voz, video y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado llevando a su vez el control de la programación de los mantenimientos preventivos realizados en estas áreas de procesamiento.

La DSI es la dependencia de la Universidad encargada de velar por la seguridad de los espacios e infraestructuras de procesamiento de información bajo los cuales se apoyan los servicios informáticos de misión crítica que utiliza la comunidad universitaria, por ende establece pautas y aprueba las solicitudes para el ingreso temporal a los espacios que están bajo su custodia, evaluando la pertinencia del ingreso y definiendo los responsables del registro y supervisión de los ingresos autorizados a sus áreas.

8.12.1 ÁREAS SEGURAS

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

8.12.1.1 Perímetro de seguridad física

Las áreas de procesamiento de datos deben cumplir con los siguientes lineamientos:

1. Todas las puertas de acceso que utilizan sistemas de control de acceso permanecen cerradas y es responsabilidad de todos los funcionarios autorizados evitar que las puertas se dejen abiertas.
2. Se deben mantener las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la infraestructura tecnológica que apoyan los servicios informáticos institucionales:
    a. Asignar personal que controle el acceso al interior del centro de procesamiento.
    b. Disponer de un puesto de recepción que autoriza y notifica el acceso.
    c. Acceso controlado por medio de tarjetas o controles biométricos.
    d. Barreras físicas de piso a techo, con puertas dobles de acceso en diferentes materiales, que soportan altas temperaturas, evitan la apertura forzada.
    e. Disponer de sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de

vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas.

f. Disponer de sistema de refrigeración de aire por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración del aire.
g. Monitorear los sistemas en mención de forma permanente y llevar un registro de los mantenimientos preventivos realizados y de los niveles de funcionamiento detectados.

3. Las instalaciones en dónde operan los centros principales de tratamiento de información deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades que se realicen en ellos.
4. Las vías de acceso deberán estar dotadas de sensores de movimiento en pasillo que controlen el encendido y apagado de la iluminación.
5. Disponer de extintores de incendios debidamente probados periódicamente, y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales.
6. Los detectores de humo o incendio deberán ser probados periódicamente de acuerdo a las recomendaciones del fabricante.
7. Establecer y separar físicamente las áreas de trabajo sobre el centro de datos, que van a ser gestionadas por personal externo y el personal propio de la DSI.
8. Proteger y separar el suministro de energía ininterrumpido del centro de datos de los otros elementos de cómputo y de red.
9. Garantizar que el centro de cómputo y los centros de cableado, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
10. En el momento de definir un espacio para área de carga o descarga, se debe garantizar que dicho espacio se encuentre aislado de los centros de datos y otras áreas de procesamiento o transmisión de información.
11. Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad
12. Es responsabilidad de todos los funcionarios de la DSI borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo, igual que no dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.
13. Las visitas a las instalaciones de procesamiento se harán en el horario autorizado por la DSI y en caso de requerir accesos en horas adicionales se solicitará la autorización del jefe de la DSI.
14. Las UAA o dependencias que tienen bajo su custodia centros de cómputo y centros de cableado deben velar por cumplir con los lineamientos expuestos en esta política, al igual que velar por suministrar las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la infraestructura tecnológica ubicada en estos sitios. Para cumplir con esto deben existir:
    a. Sistemas de control ambiental de temperatura y humedad.
    b. Sistemas de extinción de incendios.
    c. Sistemas de vigilancia y monitoreo.
    d. Alarmas en caso de detectarse condiciones ambientales inapropiadas.

e. Sistemas para el suministro de corriente contra fallas o interrupciones eléctricas.

8.12.1.2 Controles de acceso físico

1. Solo el personal autorizado por la DSI puede acceder a los centros de procesamiento o cableado.
2. Las actividades de limpieza en las áreas seguras deberán ser controladas y supervisadas por un funcionario de la DSI. El personal de limpieza deberá ser instruido acerca de las precauciones mínimas a seguir durante el proceso de limpieza y se prohibirá el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.
3. Mantener un registro del ingreso de los visitantes (registrar su fecha y hora de entrada/salida) al centro de cómputo y a los centros de cableado que están bajo su custodia.
4. Los visitantes que sean autorizados para ingresar a estos puntos con acceso restringido deberán estar siempre acompañados de un funcionario de la DSI durante su visita al centro de cómputo o los centros de cableado, o a oficinas o áreas donde se maneje información.
5. Se deberá exigir a todos los visitantes, sin excepción, que mientras permanezcan en los centros de procesamiento de información, portar la tarjeta de identificación de visitante o escarapela en un lugar visible. Así mismo, todos los funcionarios deberán portar su carnet en un lugar visible mientras permanezcan dentro de las instalaciones de procesamiento de información de la DSI.
6. El personal externo que requiera permanecer en las oficinas de DSI por periodos superiores a dos (2) días deberán ser presentados al personal de oficina donde permanecerá.
7. Revisar periódicamente y modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
8. Almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de la DSI.
9. En caso de pérdida de la tarjeta de acceso suministrada por la DSI, los responsables deben reportarlo a la mayor brevedad posible a la DSI.
10. No está permitido el ingreso de los miembros de la comunidad universitaria o terceros a áreas seguras, sin previa autorización del jefe de la DSI.

8.12.1.3 Seguridad de oficinas, despachos e instalaciones

1. Los espacios de procesamiento o tratamiento de información de la Universidad estarán protegidos con credenciales de acceso limitando el ingreso solo a personal autorizado.
2. Los espacios de procesamiento o tratamiento de información de la Universidad no estarán identificables a simple vista, tendrán una identificación limitada y audición reducida de manera tal que no dan inicio del tipo de actividad que se realiza en ellos.
3. El centro de datos principal estará dotado de un sistema de blindaje electromagnético para reducir la posibilidad de robo o daño de información por medios electromagnéticos.

4. Los planos, directorios o guías telefónicas internas que identifica la ubicación de los lugares de las instalaciones de procesamiento de información confidencial no deben estar al alcance de ninguna persona no autorizada.

8.12.1.4 Protección contra amenazas externas y del ambiente

El área que cubre el centro de procesamiento de datos institucional se encuentra protegido por una edificación antisísmica, dotado de elementos que se activarán en caso de un incendio sin dañar los dispositivos electrónicos; sin embargo, este centro de procesamiento se encuentra respaldado por un centro de datos alterno que entrará en funcionamiento en un lapso de tiempo corto en caso de falla total del centro de datos principal.

8.12.1.5 El trabajo en las áreas seguras

1. Todo trabajo que se realice por terceros sobre las áreas seguras a cargo de la DSI deberá ser supervisados por un funcionario de la DSI, por ende, queda prohibido la realización de trabajos sin supervisión por parte de esta unidad.
2. Al finalizar toda visita sobre los centros de procesamientos, se deberá realizar revisión de las zonas visitadas.
3. Si hay personal externo autorizado y realizando trabajos sin acompañamiento por personal de la UAA responsable, se debe asegurar que el acceso a otras áreas esté bloqueado y que todo el cableado esté seguro. Se aconseja realizar una inspección física de las instalaciones al finalizar los trabajos.
4. Cuando ocurra un incidente de seguridad sobre las áreas seguras, se deben suministrar los accesos al personal, solo para fines específicos, es decir que no tengan acceso a espacios no requeridos.
5. Únicamente el personal pertinente debe conocer de la existencia de las áreas seguras o de las actividades que se realizan dentro de ellas.
6. Las áreas seguras vacías deben estar cerradas con llave y serán revisadas periódicamente.
7. Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
8. Dentro las áreas de trabajo seguro se prohíben:
    a. Fumar, comer o beber.
    b. El uso de móviles / cámaras en área seguras a no ser que estén expresamente autorizados.
    c. Tocar o manipular de cualquier forma equipos instalados en áreas seguras a menos que esté específicamente autorizado para hacerlo.
    d. Conectar cualquier dispositivo eléctrico o de red a la red eléctrica o de datos, o a menos que esté específicamente autorizado para hacerlo.
    e. Archivar, depositar o guardar cualquier tipo de material que no forme parte del área segura.
    f. Guardar materiales o equipos inflamables.

g. Utilizar cualquier tipo de dispositivo de calefacción.

8.12.2 SEGURIDAD DE LOS EQUIPOS

Los lineamientos expuestos para esta política propenden por prevenir pérdidas, daños, hurtos o comprometer los activos, así como la interrupción de las actividades misionales de la Universidad.

8.12.2.1 Ubicación y protección del equipamiento

Los equipos tecnológicos que forman parte de la infraestructura tecnológica que apoyan las actividades de misión crítica de la universidad estarán resguardados con cuidados y protecciones que garanticen el funcionamiento permanente de los servicios hacia la comunidad universitaria, para ello se establece:

1. Las salidas, entradas, pérdidas y traslados de las estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales se gestionan bajo los procedimientos establecidos por la oficina de Inventario.
2. Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico de propiedad de la Universidad, el usuario responsable debe seguir los lineamientos establecidos en la política de soporte y mantenimiento de recursos y servicios informáticos, o en su defecto acudir al contratista con el cual se han establecidos contratos de mantenimiento y soporte.
3. Cuando un elemento de cómputo que forme parte de los elementos de procesamiento y transmisión de información crítica y requiera ser dado de baja, se le debe aplicar la política de borrado seguro.
4. Todos los recursos tecnológicos que forman para de los data center estarán ubicados en espacios no visibles a la comunidad y su accesibilidad es de estricta restricción solo para personal autorizado por el jefe de la DSI.
5. Colocar en un lugar visible las directrices establecidas acerca de no comer, consumir líquidos ni fumar en cercanías de las instalaciones de procesamiento de información para evitar daños o simplemente evitar que los empleados estén en contacto con los equipos si no están trabajando en ellos.
6. Hacer seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente los equipos de las instalaciones de procesamiento de información.
7. Proteger las edificaciones, en las cuales existen instalaciones de procesamiento de información, de descargas eléctricas atmosféricas y colocar filtros a todas las líneas de comunicaciones y de potencia entrante, para la protección contra dichas descargas.
8. Implementar en los elementos, que lo requieran, medidas de protección contra radiaciones para evitar daños en los dispositivos o hurto de información.

9. Ejecutar mantenimientos preventivos y correctivos, ya sea con personal interno o externo según la necesidad e idoneidad, que permitan conservar y alargar la vida útil de los recursos tecnológicos y evitar la interrupción de los servicios informáticos.
10. Contar con pólizas de seguros sobre los equipos más críticos que forman parte de la infraestructura tecnológica bajo la cual se soportan los procesamientos de información.

8.12.2.2 Elementos de soporte / Servicios de suministro

Los equipos de la Universidad se deben proteger contra fallas de suministros (energía y comunicaciones) necesarios para mantener operativas las instalaciones y los equipos:

1. Los dispositivos de suministro principal de energía que apoyan los equipos y áreas de procesamiento de información deben contar con un suministro alterno que permita el funcionamiento de los servicios mientras se restablece el suministro principal, establecimiento a su vez las condiciones de funcionamiento y el tiempo máximo que puede operar el suministro alterno. Si es posible se establecerá la alternativa de contar con un tercer suministro.
2. Disponer de un sistema de refrigeración redundante que pueda entrar en funcionamiento una vez deje de funcionar el principal.
3. Establecer canales alternativos de comunicación, sobre los servicios de la red de mayor criticidad, que les permitan a los funcionarios hacer uso de los estos servicios en caso tal de falla de los canales prioritarios.
4. Establecer convenios con entidades externas que garantice el restablecimiento y funcionamiento de los servicios en los casos más críticos.
5. Cumplir con las especificaciones de los fabricantes de los equipos en uso que permitan asegurar su adecuado funcionamiento.
6. Evaluar y registrar periódicamente las capacidades de uso de los equipos y dispositivos para estar al nivel de crecimiento de los servicios soportados.
7. Realizar pruebas de funcionamiento de los mecanismos redundantes para validar su funcionamiento apropiado.
8. Determinar la viabilidad de aplicar alarmas sobre los sistemas de suministro con la intención de anticiparse o detectar fallas de funcionamiento.

8.12.2.3 Seguridad en el cableado

La Universidad garantizará los controles necesarios para la protección del cableado de energía y de comunicaciones que afecta a los sistemas de información:

1. Separar los cables de potencia de los cables de comunicaciones para evitar interferencias.
2. Mantener los cables de red de los centros de cableados claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
3. Mantener los cuartos de cableados con acceso restringido y controlado.

4. Disponer de los planos que describan las conexiones del cableado.
5. Establecer un programa de revisiones y/o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados.
6. Establecer que las líneas de potencia y de telecomunicaciones que entran a instalaciones de procesamiento de información deben ser subterráneas en donde sea posible.
7. Mantener aislado y de forma segura los cables que estarán alrededor de las salas de procesamiento y servidores, para evitar la conexión de dispositivos no autorizados.
8. Aplicar mecanismos para asegurar y proteger el cableado de los puntos de acceso que llegan a las oficinas o a las salas de cómputo, disminuyendo las intercepciones y daños.
9. En lo posible aplicar técnicas de barrido sobre los cables de comunicación para detectar dispositivos no autorizados (bugs y sniffers) conectados al cableado.
10. En lo posible realizar instalaciones de conduit apantallado y mantener los puntos de inspección y terminación con cajas o llaves.
11. En lo posible usar blindaje electromagnético para proteger los cables.

8.12.2.4 Mantenimiento del equipamiento

La Universidad garantizará que los equipos se mantienen adecuadamente para garantizar que no se deterioren y estén siempre disponibles:

1. Es responsabilidad del funcionario velar por el funcionamiento adecuado de los equipos a su cargo e informar, en caso de detectar fallas, al equipo de soporte acogiéndose a la política de soporte y mantenimiento de recursos y servicios informáticos o en su defecto acudir al proveedor con el cual se haya adquirido algún tipo de soporte.
2. Velar porque los equipos se mantengan y operen bajo las recomendaciones y especificaciones del fabricante.
3. Velar porque los equipos críticos se mantengan con todos los requisitos exigidos por las pólizas de seguros, en caso de existir.
4. Mantener contratos de soporte y mantenimiento, en la medida de lo posible, de los equipos considerados críticos.
5. Solo personal autorizado y especializado puede realizar operaciones de mantenimiento sobre los equipos considerados críticos y mantener registros de las actividades de mantenimiento ejecutadas sobre los mismos.
6. Aplicar controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; propendiendo por restringir el acceso a la información confidencial y a no causar trauma en la prestación de los servicios.
7. Verificar que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.

8.12.2.5 Retiro de bienes

El retiro de los equipos de cómputo, de la información o del software o de cualquier otro activo de información, dentro de una UAA, se realizará teniendo en cuenta los procedimientos definidos (entrada, asignación, traslado, robo, perdida, salida, donación, devolución, baja) por la oficina de Inventario en el manual normativo y procedimental para la administración y control de los bienes muebles de la UIS, sin dejar de:

1. Obtener autorización del propietario y custodio del activo para ser retirado del área de funcionamiento por el personal autorizado.
2. Llevar un registro de los equipos retirados y de su retorno, así como de la identificación de personal que ha realizado el retiro.

8.12.2.6 Seguridad de los activos fuera de las instalaciones

El retiro de cualquier equipo o activo de información, fuera de las instalaciones de la Universidad se realizará teniendo en cuenta los procedimientos definidos (entrada, asignación, traslado, robo, perdida, salida, donación, devolución, baja) por la oficina de Inventario en el manual normativo y procedimental para la administración y control de los bienes muebles de la UIS, estableciendo a su vez:

1. Los riesgos sobre los que estarán expuestos en las instalaciones que serán usadas.
2. No dejar sin vigilancia o expuesto al público los elementos retirados de la Universidad.
3. Registros de la custodia de los activos que han salido de la Universidad.
4. La responsabilidad del retiro, uso y reintegro recae sobre el funcionario, contratista o estudiante a quién se le autoriza la custodia del equipo.

8.12.2.7 Seguridad en la reutilización o eliminación de equipos

La reutilización o eliminación de cualquier activo de información, fuera de las instalaciones de la Universidad se realizará teniendo en cuenta:

1. los procedimientos definidos (entrada, asignación, traslado, robo, perdida, salida, donación, devolución, baja) por la oficina de Inventario en el manual normativo y procedimental para la administración y control de los bienes muebles de la UIS.
2. La política de borrado o eliminación seguro de la Universidad, con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma, labor que será realizada por la División de Mantenimiento Tecnológico.

8.12.2.8 Equipamiento desatendido por el usuario

1. Los miembros de la comunidad que usen equipos de cómputo deben bloquear sus pantallas cuando estos se encuentren desatendidos (protector de pantalla protegido con contraseña)

2. Además de los procedimientos de bloqueo de pantalla, la sesión de la aplicación y de la red debe cerrarse cuando las conexiones o lo servicios no se utilizan, esto con el fin que la sesión del usuario no quede activa con los privilegios a la mano.
3. Los equipos de cómputo que estén siendo transportados, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista.
4. Si un funcionario deja el equipo desatendido con las sesiones de conexión abierta a los servicios de red, dichos sesiones de conexión serán cerradas de forma automática después de determinado tiempo.

8.12.2.9 POLÍTICA DE ESCRITORIOS Y PANTALLAS LIMPIOS

8.12.2.9.1 Sobre el Escritorio Limpio durante la jornada laboral

En vista de que las oficinas de la Universidad son visitadas frecuentemente por otros miembros de la comunidad proveedores, consultores, clientes, personal de limpieza, se establece que cada funcionario:

1. Debe mantener su escritorio lo más limpio y organizado posible, ya que, si está desordenado, es muy probable que no se dé cuenta de que le hace falta algo.
2. Retirar del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.), cuando el funcionario no permanezca en su puesto de trabajo, todos los elementos con información considerada sensible (documentos impresos, soportes de almacenamiento de datos) y archivarla de forma segura de acuerdo a lo establecido en la política de clasificación de la información, para evitar que quede al alcance o sea copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento, manteniendo presente NO publicar o dejar a la vista, documentos o datos sensitivos, por ejemplo:
    a. Nombre de Usuario y Passwords
    b. Direcciones IP
    c. Contratos
    d. Números de Cuenta
    e. Listas de Clientes
    f. Propiedad Intelectual
    g. Datos de funcionarios
    h. Cualquier información que no se deba publicar.
3. Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deberá reutilizar papel que contenga información CONFIDENCIAL.
4. Evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (escáneres, cámaras digitales).

8.12.2.9.2 Sobre el Escritorio Limpio después de la jornada laboral

1. Los funcionarios de la Universidad deberán tomarse el tiempo necesario antes de abandonar la oficina para recoger y asegurar el material sensitivo y de ser posible dejar bajo llave gabinetes, cajones y oficinas.
2. Los funcionarios al finalizar sus actividades diarias deberán cerrar todas las aplicaciones y apagar la estación de trabajo.

8.12.2.9.3 Sobre la pantalla limpia

1. Los funcionarios de la Universidad deben bloquear la pantalla de su computador con un protector de pantalla que bloquee el acceso al computador en los momentos que no esté utilizando el equipo.
2. Los funcionarios deben mantener la pantalla del equipo limpia o libre de archivos confidenciales, de manera tal que otra persona no pueda extraer información en algún descuido o en ausencia del funcionario e incluso por préstamo o uso temporal de la estación de trabajo.

8.13 POLÍTICA SEGURIDAD DE LAS OPERACIONES

La Universidad garantizará que las operaciones que se realicen sobre los recursos tecnológicos (hardware, software, instalaciones) de procesamiento de información de misión crítica se ejecuten de forma correcta y segura.

8.13.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

La DSI como la UAA encargada de gestionar los recursos tecnológicos (hardware, software, instalaciones, bases de datos) usados para el procesamiento de la información de misión crítica, ejecuta acciones que permiten velar por la integridad, disponibilidad y confidencialidad de los recursos bajo su custodia. En pro de ello la DSI requiere:

1. Elaborar y actualizar la documentación de los procedimientos relacionados con la operación y administración de la infraestructura tecnológica de la Universidad Industrial de Santander y los sistemas de información.
2. Gestionar la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la Universidad, efectuando proyecciones de crecimiento y provisiones en la infraestructura tecnológica con una periodicidad definida. La capacidad considerará proyecciones de aspectos de consumo de recursos como: procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.
3. Aplicar controles de seguridad informática y ciberseguridad a fin de resguardar los servicios tecnológicos y la información.
4. Disponer de manuales o instructivos sobre los sistemas y servicios de información que sean de interés de los miembros de la comunidad.

5. Documentar las configuraciones e instalaciones de los sistemas operativos, firmware, servicios de red, centro de datos, bases de datos, sistemas de información y demás servicios a cargo de la DSI de manera tal que se disponga de la documentación interna necesaria que permita la gestión del conocimiento de dichos recursos o servicios por parte del personal responsable.
6. Gestionar los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y acceso diferente para cada uno de los ambientes.

8.13.1.1 Gestión de cambios

Para una adecuada gestión sobre los cambios en las operaciones que se realizan sobre los recursos tecnológicos, la DSI vela por:

1. Asegurar que los cambios de alto impacto realizados sobre las instalaciones o los sistemas de procesamiento de información se realicen de forma controlada.
2. Establecer los canales sobre los cuales los funcionarios o responsables pueden solicitar cambios sobre los sistemas de información o los servicios tecnológicos (ver catálogo de servicios)
3. Establecer mecanismos que permitan determinar la trazabilidad de los cambios solicitados, aprobados/rechazados y realizados.
4. Planear los cambios sobre los sistemas de información para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los funcionarios que por sus actividades tienen relación con el sistema de información.
5. Definir los procedimientos formales para la aprobación de cambios sobre sistemas de información existentes, bien sea porque se trate de actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad del aplicativo o a los componentes que soportan el sistema de información, tales como el sistema operativo o cambios en hardware.
6. Documentar pautas para cuando se presente una situación especial para cambios de emergencia, se garantice que los cambios se apliquen de forma rápida y controlada.
7. Evaluar, con anticipación a la aplicación del cambio, los impactos potenciales que se podrían generar al aplicar un cambio, tales como aspectos funcionales y de seguridad de la información. Estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.
8. Probar los cambios realizados sobre sistemas de información e infraestructuras de red (hardware, software) para garantizar que se mantienen las condiciones de operatividad y niveles de seguridad, y que el propósito del cambio se cumplió satisfactoriamente.
9. Disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.

8.13.1.2 Gestión de la capacidad

La Universidad Industrial de Santander establece procedimientos para gestionar la capacidad de sus recursos tecnológicos para evitar pérdida de disponibilidad o rendimiento de los mismos por falta de capacidad permitiendo consecuentemente suplir necesidades actuales y anticiparse a futuras, ejecutando actividades cómo:

1. Realizar monitoreo y seguimiento de los recursos y servicios de red.
2. Planificar la ampliación de la infraestructura de red cuando sea necesario, evitando que se produzcan cuellos de botella y optimizando la prestación de los servicios de red.
3. Realizar administración del ancho de banda a servicios ávidos de recursos, dando prioridad a los más críticos para el desarrollo de las actividades misionales y realizando negación o restricción a los que no lo requieran.
4. Realizar cierre definitivo de aplicaciones, sistemas, bases de datos o ambientes que se consideran obsoletos o estén en desuso.
5. Analizar la viabilidad de ejecutar procesos por lotes fuera del horario de carga laboral.
6. Eliminar datos obsoletos o antiguos hallados en discos duros de servidores.
7. Optimizar las consultas de bases de datos o lógicas de las aplicaciones.
8. Tomar las acciones adecuadas, en la medida de lo posible, para minimizar o evitar la dependencia de elementos o personas claves para la prestación de un servicio. Entre las acciones se contemplan: redundancia de elementos, arquitecturas de contingencia o de alta disponibilidad, técnicas de gestión de conocimiento sobre la operatividad de la infraestructura, etc.

8.13.1.3 Separación de los ambientes para desarrollo, prueba y operación

La Universidad por medio de la DSI establece procedimiento para la gestión de los ambientes de desarrollo, prueba y operación, separándolos para reducir los riesgos de falla en los servicios, de acceso o cambios no autorizados al ambiente de operación:

1. Establece que el software de desarrollo y de operaciones se ubicarán y funcionarán en diferentes sistemas o procesadores de computador y en diferentes dominios o directorios.
2. Define y documenta las reglas para la transferencia de software del ambiente de desarrollo al de operaciones para las aplicaciones que lo permitan.
3. Define que los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales.
4. Define en qué circunstancias excepcionales, únicamente, las pruebas no se deben llevar, a cabo en los sistemas operacionales.
5. Define si los datos sensibles no se deben copiar en el ambiente del sistema de pruebas, y en caso tal que se copien se deben aplicar controles equivalentes del sistema de operación al sistema de pruebas, determinando a su vez la necesidad o no, de establecer acuerdos de confidencialidad.

6. Establece que los usuarios deben usar diferentes perfiles de usuario para sistemas operacionales y de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error.
7. Establece que los cambios en los sistemas en producción que involucren aspectos funcionales deben ser informados y consultados con el(los) proceso (s) propietario(s) de la información.
8. Establece que no está permitido el uso de compiladores, código fuente, editores y herramientas de desarrollo o utilitarios del sistema, en entornos de sistemas de producción cuando no se requiere, para evitar problemas de seguridad
9. Establece no realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.
10. Aplica controles a las cuentas de los desarrolladores, ya que se encuentra en una posición privilegiada, para evitar que introduzcan código malicioso o simplemente código no probado.
11. Estable un mecanismo para controlar la migración del código fuente al entorno operativo para evitar errores en el manejo de versiones antiguas o inestables.

8.13.2 SOFTWARE MALICIOSO

La Universidad Industrial de Santander por medio de la DSI aplica controles para que la información y las instalaciones de procesamiento de información se encuentren protegidas contra amenazas causadas por código malicioso.

8.13.2.1 Protección y controles ante software malicioso

1. La infraestructura de Seguridad que protege a la infraestructura de procesamiento de información de la Universidad, es del tipo UTM (Unified Thread Management/Gestión Unificada de Amenazas) en las que se cuenta con IPS- Anti-Virus, Anti-Bot, Anti Spam, ACL definido por segmentación de red para garantizar los mínimos privilegios garantizados, con el fin de mitigar el riesgo de ejecución de virus o códigos maliciosos. Así mismo, se restringirá la ejecución de aplicaciones y se mantendrá instalado y actualizado un sistema de antivirus, en todas las estaciones de trabajo y servidores de la Universidad que estén a cargo de la DSI.
2. Los usuarios de los servicios de red ofrecidos por la DSI son responsables de la utilización y actualización de programas antivirus en los dispositivos que usan para conectarse a la red, con el fin de analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos y/o removibles y/o los archivos y/o el correo electrónico que esté autorizado a utilizar para el desarrollo de sus funciones.
3. Los funcionarios, mediante el uso del software de antivirus, deben verificar que todo archivo, independiente de su procedencia, esté libre de virus antes de ser accedido.
4. Ningún miembro de la comunidad o tercero debe descargar software desde sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la DSI.
5. Los miembros de la comunidad o terceros que sospechen de alguna infección por virus deben notificar a la DSI, para la revisión y eliminación del virus.

6. Ningún miembro de la comunidad o tercero debe realizar modificaciones o eliminar las configuraciones de seguridad en Antivirus, Outlook, office, navegadores u otros programas, para detectar y prevenir la propagación de virus, que se han dispuesto en los equipos de cómputo institucional.
7. La adecuación de nuevas estaciones de trabajo o servidores que realicen actividades para el propósito misional deben contar con un programa de antivirus previo a la instalación de cualquier otro programa sobre el sistema operativo.
8. Los servidores o servicios de red que se implementen en las UAA deben disponer de un administrador que vele por la seguridad del mismo y por estar dentro la infraestructura de red de la Universidad, la DSI se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, tramitan o trasporten con el fin de detectar riesgos de navegabilidad e infección o ataques por códigos maliciosos.
9. Se debe actualizar periódicamente las versiones de los componentes de los diferentes sistemas de seguridad operativos, incluidos, motores de detección, bases de datos de firmas, software de gestión en el lado cliente y servidor, etc.
10. Las estaciones de trabajo institucional deben contar con el programa antivirus, aprobado por la DSI, que permita protegerlas de virus y/o código malicioso y el custodio de dichas estaciones velará por solicitar la instalación respectiva.
11. La instalación de los programas antivirus debe ser solicitada únicamente ante la DSI y deberán permanecer activos durante su uso.
12. Las UAA deben validar de forma periódica el uso de software no malicioso en las estaciones de trabajo y servidores a cargo. Esta labor se debe programar de forma automática con una periodicidad semanal.
13. Los funcionarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus y/o de detección de código malicioso, en los equipos o sistemas en que estén instalados.
14. La DSI dispondrá de mecanismos para analizar, detectar y restringir el software malicioso que provenga de posibles fuentes de código malicioso, entre ellas: descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.
15. La DSI divulgará notificaciones o boletines informativos acerca de las formas de reconocer malware, hoax, spyware, etc., con el fin de promover una cultura de seguridad de la información entre los funcionarios de la Universidad.
16. Los funcionarios podrán consultar a la DSI sobre el tratamiento que debe darse en caso de sospecha de malware.
17. Cada usuario es responsable por la destrucción de todo archivo o mensaje, que le haya sido enviado y cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la DSI (dsi@uis.edu.co) con la frase “correo sospechoso” en el asunto.

8.13.3 RESPALDO DE LA INFORMACIÓN

La Universidad evitará la pérdida de datos mediante la aplicación de una política de copias de seguridad que permita asegurar la disponibilidad e integridad de la información ante incidentes sobre los activos de información de misión crítica a cargo de la DSI y alojados en el data center principal.

8.13.3.1 Realización y restauración de copias de seguridad

1. Establecer la periodicidad con la que se harán las copias
2. Definir el alcance y nivel de las copias de seguridad sobre los datos e información sensible, el software y aplicaciones, los datos de configuración de aplicaciones sistemas etc., datos sobre accesos, claves etc., registros de actividades, eventos, mensajes o alarmas del sistema, produciendo registros exactos y completos de las copias de respaldo.
3. Documentar y llevar a cabo las pautas para realización de copias de seguridad según la guía de copias de seguridad.
4. Guardar las copias de seguridad realizadas en un lugar remoto o externo del campus principal a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en él, además deben estar restringidas de accesos no autorizados, manteniendo el nivel de confidencialidad e integridad, y las condiciones ambientales adecuadas para evitar su deterioro (según las normas aplicadas y las especificaciones dadas por el fabricante), daño, alteración o hurto.
5. Mantener el registro de las copias de seguridad como parte de un cronograma o plan de mantenimiento de copias de seguridad. También es aconsejable mantener un registro de las pruebas de validez de dichas copias.
6. Definir si las copias de respaldo estarán protegidas por medio de encriptación.
7. Verificar que las copias de seguridad se ejecuten correctamente y de acuerdo al tipo y frecuencia acordados.
8. Los administradores de las Bases de Datos, de los servidores y de los sistemas de información, son los responsables de definir la frecuencia de respaldo, el tipo, el medio de almacenamiento y los requerimientos de seguridad de la información. Estos aspectos de configuración se deben registrar en el formato de Control Copia de seguridad.
9. Garantizar la aplicación de las Tablas de Retención Documental TRD y Tablas de Valoración Documental TVD en la realización de las copias de seguridad de series y subseries documentales, teniendo en cuenta los tiempos de retención y la disposición final establecidas en este instrumento archivístico.
10. La DSI determinará los roles de usuario que intervienen dentro del proceso de copias de seguridad, según su responsabilidad y tareas:
    a. Administrador de copias de seguridad: persona encargada de realizar las copias de seguridad.
    b. Transportador: encargado de llevar las copias de seguridad fuera de las instalaciones de la institución.
    c. Probador: Encargado de probar copias de seguridad cada cierto período de tiempo.

Restauración:

1. Definir y documentar las pautas para restauración de las copias de seguridad
2. Validar que las copias son válidas permitiendo restaurar convenientemente la integridad de los datos respaldados mediante un proceso de restauración simulado o en su defecto en equipos de pruebas.
3. Documentar las pruebas de restauración en el cual se expongan los aspectos técnicos resultantes de las pruebas. Las pruebas se deben registrar en un formato de Control de Restauración de Información y se realizará por lo menos una cada doce meses.
4. Validar la integridad y accesibilidad de las cintas magnéticas por lo menos cada dos meses.
5. Definir el procedimiento para borrar físicamente la información de los medios de almacenamiento, antes de desecharlos.
6. Realizar mantenimientos sobre los medios y dispositivos para mantenerlos en buen estado y que permitan la restauración de las copias cuando se necesiten.
7. El software de restauración utilizado para recuperar las copias de seguridad debe permitir restauraciones parciales, si los niveles de integridad de los servicios lo permiten, de los datos sin obligar a la restauración de toda la información de acuerdo a los impactos de los incidentes.
8. Determinar los tiempos requeridos para realizar una restauración completa de los sistemas y datos.
9. La Universidad proporcionará los recursos y medios de respaldo adecuados para asegurar que la información esencial y el software asociado se puedan recuperar después de una falla.

8.13.4 REGISTRO Y SUPERVISIÓN

Los accesos de los usuarios a la infraestructura de red, a los sistemas, a la red de datos, a las bases de datos y a las aplicaciones a cargo de la DSI deben ser registrados según los lineamientos acordados entre los propietarios de estos y los custodios de los mismos, con el fin de permitir el monitoreo o trazabilidad de las acciones llevadas a cabo por los usuarios.

8.13.4.1 Registro de eventos

Los administradores de los recursos de la infraestructura de seguridad de la red de datos, de las bases de datos y tablas, de los sistemas operativos y de consolas de antivirus, registrarán los accesos de los diferentes usuarios que navegan o hacen uso de los servicios de la red, activando los log de auditorías de eventos considerados sensibles y serán revisados con regularidad.

Los propietarios de los diferentes sistemas de información en corresponsabilidad con la DSI y atendiendo los estándares de desarrollo seguro, definirán:

1. Los datos o actividades sobre los cuales se aplicarán los eventos de trazabilidad,
2. El alcance de la aplicabilidad de las normas legales sobre la protección de datos personales gestionados por los sistemas de información como clasificada o reservada.

3. Los ajustes a los desarrollos para implementar los controles necesarios para registrar en los logs de auditoría a los eventos acordados.

Los registros a recopilar sobre los servicios de red institucional, que lo permitan, contendrán aspectos mínimos, como:

1. Identificación de los usuarios.
2. Los intentos de acceso exitosos y rechazados.
3. Fecha y horas de entrada y salida.
4. Alertas accionadas según el de control de acceso establecido.
5. Transacciones ejecutadas por los usuarios sobre los eventos claves definidos previamente.
6. Fecha y hora en que se producen los eventos.
7. Identificación y ubicación del dispositivo, si es posible, e identificador del sistema.

Posterior al registro de los eventos, es necesario realizar revisión y análisis de dichos registros con el propósito de detectar potenciales actividades fraudulentas, o detectar el origen de fallos de funcionamiento, antes de que ocurran incidentes importantes:

1. Los administradores de seguridad perimetral deben revisar en la periodicidad establecida los reportes generados por la plataforma e identificar intentos de accesos no autorizados con su correspondiente cantidad de eventos, origen y tipo de evento (firewall, ips, waf, rdp, vpn, acceso a plataformas de gestión, otros componentes tecnológicos para la seguridad y telecomunicaciones).
2. Los administradores de consola de antivirus deben revisar los reportes generados por la plataforma e identificar anomalías en cada uno de los servidores y estaciones de trabajo generando un consolidado de amenazas identificadas.
3. El responsable de la infraestructura de seguridad de la red de datos, recopilará y revisará los resultados de los reportes generados por los motores de las bases de datos, aplicaciones, sistema operativo y consola de antivirus, correo electrónico con la finalidad de presentar propuestas de acciones y formular ajustes necesarios para la solución de las alarmas o incongruencias identificadas.
4. Los responsables de gestionar los activos de información digital involucrados, deben revisar log´s de auditoria generados o reportados por el responsable de la seguridad de la red de datos según el correlacionador de eventos.

8.13.4.2 Protección de la información de registros (logs)

1. La DSI garantizará que la información generada por los logs o eventos monitoreados, serán protegidos y guardados cuidadosamente para evitar el acceso o manipulación no autorizada.
2. Los profesionales de la DSI, no están facultados para modificar, borrar o desactivar registros (logs) de sus actividades propias, ni de los usuarios de los sistemas de información e infraestructura de red, de igual forma se deben realizar las configuraciones de seguridad necesarias para evitar la eliminación o cambios no autorizados a los registros de información.

3. El acceso a los registros (logs) es restringido, por lo cual su consulta por usuarios se debe realizar con previa autorización de la DSI.
4. La consulta y copia de la información de registros que se requiera con fines probatorios debe ser solicitada por la oficina de control interno disciplinario
5. La DSI definirá y ejecutará las tareas de revisión de logs de eventos y auditando periódicamente los registros de actividades (logs) de los administradores de los sistemas de información y telecomunicaciones
6. Los logs deben tener mecanismos de seguridad y control administrativo resistentes a ataques para evitar la adulteración de los mismos, también deben generar las capacidades suficientes para detectar y
7. La DSI junto con la Dirección de Certificación y Gestión Documental y la UAA responsable de la información pertinente, determinarán los períodos de retención de los registros (logs) de auditoria de los recursos tecnológicos y los sistemas de información institucional.
8. Implementar en los desarrollos de software, los controles necesarios para generar y garantizar la integridad los registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los sistemas de información desarrollados.
9. Implementar en los desarrollos de software mecanismos para registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros.
10. Verificar cuando se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobre escritura de eventos pasados registrados.

8.13.4.3 Registros del administrador y operador

1. Se deben registrar las actividades no solo de los usuarios sino también de los administradores, teniendo especial cuidado con los que tienen privilegios de administración dado el riesgo que tiene si pueden acceder a los registros y manipularlos o borrarlos.
2. Todas las actividades de operación realizadas por los administradores sobre la infraestructura tecnológica y de procesamiento de información de la DSI (Servidores, Red de datos, Sistemas de información) deberán estar debidamente registradas.
3. Los administradores de la infraestructura de procesamiento de información tendrán asignada una cuenta de usuario única, a través de la cual se realizarán las actividades de administración.

8.13.4.4 Sincronización de relojes

1. La DSI mantendrá un servidor de tiempo (NTP – Network Time Protocol) que deberá ser utilizado para la sincronización en tiempo de todos los equipos de la red LAN institucional, por lo tanto, todas las UAA que lo requieran deberán sincronizar sus equipos con este servidor.

2. El administrador del servidor de sincronización garantizará la disponibilidad de estos servicios para las UAA que lo requieran.

8.13.5 CONTROL DE SOFTWARE EN PRODUCCIÓN

La DSI velará por la integridad de los sistemas operacionales que estén bajo su custodia y administración.

8.13.5.1 Instalación de software en sistemas operativos u operacionales

1. La DSI designará responsables y establecerá procedimientos para controlar la instalación de software en los equipos informáticos e infraestructura de procesamiento de información y se cerciorará de contar con el soporte de los proveedores de dicho software/hardware y asegurará la funcionalidad de los sistemas operacionales que operan sobre la infraestructura tecnológica cuando el software sea actualizado.
2. Se establece que las actualizaciones de aplicaciones, bibliotecas, librerías y software operativo se llevarán a cabo únicamente por el líder funcional encargado de administrar los servidores o en su defecto el funcionario entrenado y autorizado por la DSI y basándose en los lineamientos de control de cambios existentes.
3. Se establece que los sistemas operativos sólo deben contener códigos ejecutables aprobados, no el código de desarrollo o compiladores.
4. Se establece que las aplicaciones y el software de los sistemas operacionales solo se deben implementar después de pruebas exitosas; los ensayos se deben realizar en sistemas separados y abarcan aspectos como la usabilidad, la seguridad, los efectos sobre otros sistemas; también se debe asegurar que todas las bibliotecas de fuentes de programas correspondientes hayan sido actualizadas antes de la implementación.
5. Se establece implementar un mecanismo para documentar el software implementado.
6. Se establece una estrategia de retroceso (rollback) antes de implementar los cambios.
7. Se establece mantener un log de auditoría de todas las actualizaciones de las bibliotecas de programas operacionales.
8. Se establece un mecanismo para controlar el versionado del software de aplicación de manera tal que se conserven las versiones anteriores como una medida de contingencia.
9. Se establece que las versiones de software anteriores se deben llevar al archivo permanente, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores, en tanto los datos permanezcan en el archivo permanente.
10. Se establece garantizar que el software operativo instalado en la infraestructura tecnológica de la red institucional cuenta con soporte de los proveedores.
11. Se establece conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
12. Se establece validar los riesgos que genera la migración hacia nuevas versiones del software operativo.
13. Se establece mantener un inventario del software implementado, así como sus respectivas versiones y niveles de soporte por parte del proveedor.

8.13.6 GESTIÓN DE VULNERABILIDAD TÉCNICA

Los controles establecidos a continuación propenden por gestionar las posibles vulnerabilidades técnicas que se pueden presentar en las infraestructuras de procesamiento de información y servicios de red a cargo de la DSI con el fin de identificarlas y prevenir su explotación por algún atacante. Para ello, la gestión de vulnerabilidades técnicas estará basada en diferentes estrategias:

1. Monitoreo permanente sobre la infraestructura tecnológica y los servicios de red.
2. Seguimiento permanente a los reportes de fabricantes y proveedores de los equipos que forman parte de la infraestructura informática que están bajo la responsabilidad directa de la DSI.
3. Seguimiento de los servicios de seguridad informática contratados.
4. Realización de pruebas periódicas de vulnerabilidades y hacking ético.
5. Seguimiento y atención de los reportes de usuarios internos y externos sobre posibles eventos de seguridad.

8.13.6.1 Gestión de vulnerabilidades técnicas

La Universidad establece las siguientes directrices para el tratamiento de vulnerabilidades técnicas:

1. Cada UAA debe realizar el levantamiento del inventario de activos de información, bajo su custodia, monitorearlos, identificar sus riesgos y documentar los posibles controles a implementar según el tipo de vulnerabilidad técnica que se pueda presentar.
2. Establecer el equipo de respuestas a incidentes al interior de la DSI, el cual será el responsable de identificar y gestionar las vulnerabilidades técnicas potenciales relacionadas con los activos de información de misión crítica a su cargo. De acuerdo a ello el equipo:
    a. Realizará el seguimiento y evaluación regular sobre la vulnerabilidad identificada, la valoración de riesgos de la vulnerabilidad, la colocación de parches o la implementación de controles pertinentes, la valoración de los controles para asegurar su eficiencia y eficacia; si no es posible implementar controles a las vulnerabilidades identificadas, se debe documentar en los riesgos de acuerdo a su probabilidad e impacto y colocarlo como riesgo aceptado.
    b. Consultará foros especializados en la gestión de vulnerabilidades según los activos de información a su cargo.
    c. Mantendrá actualizada la información de fabricantes y proveedores según los activos de información.
    d. Coordinará las pruebas de ataques simulados (hacking ético) según el activo de información a cargo. En lo posible gestionará para que las pruebas se realicen por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.
    e. Realizará escaneos periódicos de vulnerabilidades

f. Definirá los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y mantendrá un nivel de conciencia acerca de los riesgos si se llegasen a materializar la explotación de las vulnerabilidades
g. Establecerá una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes.
h. Definirá, dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción a tomar y dicha acción se debería llevar a cabo de acuerdo con los controles relacionados con la gestión de cambios, o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información.
i. Ante una vulnerabilidad técnica, evaluará y probará la eficacia de parches de seguridad, antes de su instalación, determinando que no se producen efectos secundarios que no se puedan tolerar; si no hay parches disponibles, se debe considerar otros controles como:
    i. Suspender los servicios o capacidades relacionados con la vulnerabilidad;
    ii. Adaptar o adicionar controles de acceso (cortafuegos, en los límites de la red)
    iii. Incrementar el seguimiento para detectar ataques reales
    iv. Tomar conciencia sobre la vulnerabilidad.
j. Llevará un log de auditoría para todos los procedimientos realizados.
k. Abordará primero los sistemas que están en alto riesgo.
l. Establecerá un proceso de gestión eficaz de la vulnerabilidad técnica alineada con las actividades de gestión de incidentes para comunicar los datos sobre vulnerabilidades a la función de respuesta a incidentes y suministrar los procedimientos técnicos para realizarse en caso de ocurrir un incidente.
m. Definirá un procedimiento para hacer frente a una situación en la que se ha identificado una vulnerabilidad, pero no hay una contramedida adecuada. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las acciones de detección y correctivas apropiadas.

8.13.6.2 Restricciones en la instalación de software

La Universidad Industrial de Santander a través de sus UAA determina las aplicaciones y software que requieren los funcionarios para el desempeño de sus funciones, y en vista de ello se establece el cumplimiento de las siguientes directrices para limitar la instalación de software por parte de los usuarios:

1. Queda prohibido la instalación o desinstalación de software por parte de los usuarios sin el conocimiento del jefe inmediato o responsable de la UAA.
2. El jefe de cada Unidad Académico Administrativas debe garantizar que los funcionarios y/o proveedores hagan uso adecuado de los equipos suministrados y evitar que se realice la instalación de software libre o no licenciado en contravía de la política establecida y de los derechos de autor o de propiedad intelectual.

3. La DSI solo presta el servicio de instalación y configuración de aplicaciones de software que se encuentran cubiertas bajo el licenciamiento del campus agreement, por ende, cualquier funcionario puede solicitar la instalación/desinstalación de dichas aplicaciones teniendo en cuenta los requisitos e indicaciones expuestas en el catálogo de servicios.
4. Las UAA que adquieren licencias de software, tienen bajo su responsabilidad el uso, instalación y desinstalación de las mismas de acuerdo al número de licencias adquiridas y las condiciones expuestas por el proveedor y fabricante.
5. La DSI divulgará la lista actualizada del software a su cargo y que está disponible para uso de las diferente UAA, al igual que las condiciones de uso.
6. Los usuarios podrán instalar las actualizaciones y parches de seguridad de los sistemas operativos y software antivirus instalados en sus equipos.
7. No está permitido que los usuarios desinstalen, modifiquen o inactiven los antivirus o las actualizaciones de seguridad correspondiente a los sistemas operativos.

8.13.7 CONSIDERACIONES SOBRE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

La Universidad Industrial de Santander por medio de la oficina de Control Interno y Evaluación de Gestión definen las pautas para auditar, de manera interna, los controles que la DSI o UAA aplican sobre sus activos de información para proteger la integridad, disponibilidad, confidencialidad de la información.

De manera complementaria, la DSI como unidad responsable de los servicios informáticos institucionales de misión crítica, puede solicitar la realización de auditorías a entes externos con idoneidad en el área a auditar con el propósito de tener certezas sobre los controles aplicados que le garanticen a la institución la seguridad de la información y la disponibilidad de los servicios de red y de acuerdo a los hallazgos de vulnerabilidad aplicar nuevos controles o ajustar los actuales; permitiendo obtener hallazgos en relación a si:

1. Los usuarios están trabajando con los privilegios correctos.
2. La infraestructura es estable y confiable.
3. Las infraestructuras cuentan con la suficiente capacidad (memoria, procesamiento, almacenamiento, ancho de banda).
4. Las pruebas realizadas son efectivas.
5. Las actividades de mantenimiento, monitoreo y gestión son efectivas.
6. Las actividades de los usuarios de los sistemas se ejecutan según los lineamientos establecidos.

En el momento de realizar actividades de auditoría técnica se tendrán en cuenta aspectos como:

1. Definir el alcance de la auditoria.

2. Determinar si las auditorias producirán un impacto sobre el desempeño de los servicios para así seleccionar un horario no laboral para realizarlas.
3. Brindar apoyo técnico al responsable de la auditoria para facilitar las actividades planificadas.
4. Establecer acuerdos de confidencialidad en los casos considerados necesarios.
5. Limitar el acceso al personal auditor solo a los espacios y áreas autorizadas.

8.14 SEGURIDAD DE LAS COMUNICACIONES

La Universidad velará para que la información que se transmite a través de la infraestructura de la red de datos institucional se realice por canales y dispositivos de comunicación seguros. Para ello establece:

8.14.1 POLÍTICA GESTIÓN DE LA SEGURIDAD DE RED

La DSI es la Unidad encargada de aplicar los controles que propendan por asegurar la protección de la información en las redes y los recursos de procesamiento de la información que están bajo su custodia y administración.

8.14.1.1 Controles de Red

Para gestionar y controlar la red institucional, la DSI deberá:

1. Establecer los roles, procedimientos y controles para la gestión de los equipos y servicios de la red de datos.
2. En la medida que sea posible y practicable, establecer que los funcionarios que tienen a cargo la responsabilidad operacional de la red de datos y/o de los sistemas informáticos institucionales, operen de forma segregada.
3. Establecer controles especiales para proteger los sistemas de información y la disponibilidad de los servicios y dispositivos de red.
4. Establecer mecanismos para el monitoreo de acciones y registro de la autenticación de inicio de sesión, sobre servicios de red o tecnológicos que se consideren relevantes para la seguridad de la información. Por ejemplo: WIFI, sistemas de información.
5. Promover acciones de concienciación sobre el uso adecuado de la información de los servicios y de la infraestructura de red, con el fin de evitar o reducir los incidentes relacionados con la seguridad y privacidad de la información.
6. Establecer y dar a conocer los mecanismos de control acceso de los usuarios cuando estos requieran acceder a servicios institucionales desde redes públicas o inalámbricas con el fin de salvaguardar la protección de los datos, tal como VPN entre otros.
7. Implementar los mecanismos informáticos para proteger de forma segura el tráfico de los paquetes de información que se transmiten sobre la red de datos contra ataque

informático, introducción o propagación de software malicioso, interceptación, copiado, modificación, enrutado y destrucción.

8. Incrementar paulatinamente, cuando sea técnica y financieramente viable, el nivel de seguridad de control de acceso, al de las simples contraseñas, en los servicios que lo permitan, como por ejemplo uso de teléfono móvil, ID de huella digital, tarjetas de acceso, u otros; evitando así accesos no autorizados, aunque se conozca la contraseña.
9. Aplicar restricción a las conexiones de red para que los accesos se realicen según los privilegios asignados.
10. establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red, acogiendo buenas prácticas de configuración segura.
11. Implementar firewall o dispositivos de seguridad perimetral para la conexión a internet.
12. Instalar protección entre las redes internas, de conformidad con la tecnología e infraestructura disponibles
13. Considerar y tratar como información confidencial, la información institucional relacionada con las topologías, configuraciones, direccionamiento, enrutamiento, diseños de sistemas de comunicación y de cómputo.

8.14.1.2 Seguridad de los servicios de red

La Universidad a través de la DSI definirá la tecnología y el conjunto de controles lógicos y físicos a aplicar para garantizar la seguridad sobre los diferentes recursos y servicios informáticos (autenticación, encriptación y controles de conexión de red), con el fin de asegurar el buen uso de los mismos y mantener los niveles de seguridad establecidos de conformidad con la disponibilidad de recursos presupuestales. Para ello:

1. La DSI independientemente de si los servicios de red son internos o externos (subcontratados), definirá los requisitos en relación a la calidad del servicio mediante acuerdos de Niveles de Servicio o SLA.
2. La DSI realizará monitoreo sobre el tráfico de la red, auditando la disponibilidad de la red y evaluando los riesgos a los que pueda estar expuesto dicho servicio y los que se ofrecen por medio de él.
3. La DSI definirá los parámetros técnicos requeridos para la conexión segura sobre con los servicios de red, de acuerdo con las normas de conexión de seguridad y de red.
4. La DSI establecerá las responsabilidades y procedimientos para la gestión de las comunicaciones que se realizan sobre infraestructura de la red de datos a los cuales se acogerán los usuarios de los servicios de red de todas las UAA.
5. La DSI definirá las situaciones y los procedimientos a aplicar para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.
6. Las UAA que requieran desplegar servicios sobre la de red deberán identificar, habilitar y justificar ante la DSI la necesidad de los servicios, protocolos y puertos que requieran, y acatarán los lineamientos de seguridad establecidos por la Universidad.
7. La DSI definirá los controles y restricciones asociadas con el reenvío automático de correo electrónico a direcciones de correo externas.

8.14.1.3 Separación en redes

1. La DSI establecerá un esquema de segregación de las redes con el fin de controlar el acceso a los diferentes segmentos de red de acuerdo a los dominios, grupos de servicios, roles y ubicación de los funcionarios. El tráfico entre estos segmentos de red estará controlado mediante elementos de red que permitan una autorización a un nivel de detalle específico (Dirección IP, puerto, otros).
2. La DSI separará las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.

8.14.2 POLÍTICA INTERCAMBIO DE INFORMACIÓN

La Universidad define que el INTERCAMBIO DE INFORMACION es toda acción que permita entrar o recibir información tanto a nivel externo como interno por parte de los funcionarios o contratistas, en el ejercicio de sus funciones u obligaciones institucionales. En virtud de ello la UAA y sus funcionarios velarán por que la información que se intercambia al interior de la Universidad e incluso con entidades externas, se realice en forma segura de conformidad con lo siguiente:

8.14.2.1 Gestión de intercambio de información.

Para una adecuada gestión del intercambio de información institucional de manera segura, velando por su confidencialidad, integridad y disponibilidad, la Universidad establece que:

1. Para el envío o recepción de información institucional se utilizarán únicamente los mecanismos y herramientas proporcionadas por la Universidad, teniendo en cuenta que el intercambio de información está sujeta a requisitos legales y reglamentarios, dependiendo de su nivel de confidencialidad.
2. Se requiere etiquetar la información a intercambiar, de acuerdo a su nivel de accesibilidad en caso de ser considerada como confidencial o reservada.
3. En caso de pérdida o extravío de datos o información institucional considerada confidencial o sensible, se deberá informar a la Oficina de Control y Evaluación de Gestión, realizar las denuncias ante las autoridades competentes y acatar los lineamientos emitidos por el Archivo General de la Nación según acuerdo 007 de octubre 15 de 2014, para la pérdida total, parcial y reconstrucción de expedientes.
4. No se deben dejar mensajes con información confidencial, en contestadores electrónicos o impresoras ya que éstos pueden ser escuchados o utilizados por personal no autorizado.
5. Los comentarios de índole personal que se intercambien con miembros de la comunidad universitaria no expresan ni comprometen el pensamiento y sentir institucional.
6. La comunidad universitaria cumplirá, según su rol institucional, con las directrices y procedimientos definidos por la Universidad para el intercambio de información de manera segura, tales como:
    a. Transferencia de información institucional ya sea a nivel interno o externo, teniendo en cuenta los niveles de clasificación de la misma (publica, reservada, clasificada) y aplicar los controles pertinentes para salvaguardarla.

b. Gestión de la información institucional física o electrónica, incluidos mensajes electrónicos, de acuerdo con la legislación y reglamentaciones locales y nacionales.
c. Detección y protección ante software malicioso que podría presentarse por el intercambio de información.
d. Uso de las instalaciones o recursos definidos para la comunicación, procesamiento e intercambio de datos o información.

7. Los funcionarios, estudiantes, contratistas y terceros acatarán las disposiciones y lineamientos definidos por la Universidad para la gestión de las comunicaciones, so pena de incurrir en las faltas a que haya lugar.

8.14.2.2 Acuerdos de intercambio/transferencia de información.

Las UAA responsables establecerán, cuando lo consideren pertinente, en los contratos y convenios que se suscriban con terceros, los acuerdos de intercambio seguro de información dejando explícitos aspectos cómo:

1. Las responsabilidades sobre el control, envío y recepción de la información entregada por la Universidad.
2. Los mecanismos para el seguimiento a la trazabilidad de los datos y el no repudio.
3. El cumplimiento de las normas técnicas y reglamentarias para el transporte y etiquetado de la información de acuerdo a su nivel de accesibilidad.
4. Los requisitos de cifrado en caso de ser necesario.
5. Las responsabilidades y obligaciones en caso de incidentes de seguridad de la información, como la perdida de datos.
6. Aplicación de controles de acceso a la información
7. Las implicaciones civiles y penales por el incumplimiento de los aspectos definidos en el acuerdo.
8. La necesidad de destruir la información una vez se cumpla con el objetivo del contrato o convenio.

8.14.2.3 Mensajería electrónica.

La Universidad Industrial de Santander, entendiendo la importancia de la información que se puede generar y compartir tanto al interior como hacia el exterior de la Universidad, por medio de las herramientas de mensajería electrónica institucional, define:

1. Ofrecer un servicio idóneo que permita garantizar la operación segura de las comunicaciones que se adelanten por los medios de mensajería electrónica institucionales, en concordancia con las políticas sobre uso y manejo de los correos electrónicos, redes sociales y servicios de colaboración, entre otros.
2. Generar y divulgar los procedimientos respectivos para el uso de los servicios de mensajería electrónica que se encuentra bajo la administración y custodia de la DSI
3. Garantizar que las plataformas de mensajería electrónica bajo la administración de la DSI, cuente con los procedimientos y controles necesarios que permitan detectar y proteger la integridad de información que viaja a través de estas plataformas.

4. Aplicar mecanismos que permitan mitigar la intrusión de software malicioso ocasionado por la recepción / envío de mensajes electrónicos realizados desde los recursos institucionales.
5. Generar campañas de concientización en los usuarios (profesores, administrativos, estudiantes, etc.), respecto a las precauciones que deben adoptar en el intercambio de información al usar los recursos institucionales de mensajería electrónica.
6. Los mensajes de chat expresados en redes sociales o herramientas de mensajería instantánea usando las cuentas de correo institucional o espacios en representación de la Universidad, deben ser expresados con respecto dando a conocer solo información institucional y no deben representar la posición del funcionario, quedando bajo la responsabilidad de la UAA a la cual pertenece el funcionario.
7. Los miembros de la comunidad y terceros no deben enviar bajo ninguna circunstancia, por medio de los recursos de mensajería electrónica institucional, archivos que contengan extensiones ejecutables con contenido malicioso.
8. La mensajería electrónica comprende los mensajes de chat electrónico, así como redes sociales para los cuales se aplicarán los numerales anteriores cuando sea pertinente.

8.14.2.4 Acuerdos de confidencialidad y de no divulgación.

1. La Universidad por medio de las UAA establecerá con los funcionarios, proveedores y contratistas a su cargo acuerdos de confidencialidad cuando estos tengan acceso a activos de información que así lo requieran.
2. Los acuerdos de confidencialidad deben constar por escrito y serán suscritos con anterioridad al inicio de una transferencia de información.
3. Los acuerdos que se establezcan deben contener, según la necesidad, entre otros, aspectos como:
    a. La información que se va a proteger (información confidencial)
    b. La duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente.
    c. Las acciones requeridas cuando termina el acuerdo.
    d. Las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información.
    e. La propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial.
    f. El uso permitido de información confidencial y los derechos del firmante para usar la información.
    g. El derecho a actividades de auditoría y de seguimiento que involucran información confidencial.
    h. El proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial.
    i. Los plazos para que la información sea devuelta o destruida al cesar el acuerdo.
    j. Las acciones que se esperan tomar en caso de violación del acuerdo.

8.15 POLÍTICA SOBRE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

8.15.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

La DSI es la dependencia de la Universidad encargada de desarrollar sistemas de información, aplicaciones o software, para el soporte de los procesos institucionales y la atención de las necesidades de las diferentes Unidades Académico Administrativas, por ende, la DSI velará por que la seguridad de la información sea una parte integral de los sistemas de información en todo su ciclo de vida.

En los casos de desarrollo subcontratado con terceros, las UAA solicitarán concepto técnico, asesoría y acompañamiento a la DSI, sobre los requerimientos, especificaciones, licenciamientos y compatibilidades de las posibles adquisiciones en relación a los ambientes, arquitectura y lenguajes de desarrollo institucional.

8.15.1.1 Análisis y especificación de los requisitos de seguridad

La DSI al construir y modificar sistemas de información o al implementar nuevos módulos a los sistemas de información existentes, definirá aspectos que permitan prever rediseños de los sistemas en las fases posteriores del ciclo de vida del desarrollo, para ello realizará a) un análisis detallado de los requerimientos en relación a la seguridad de los sistemas de información, b) un análisis de riesgos determinando posibles escenarios de riesgos y controles para mitigar los mismo.

Dentro de los controles a tener en cuenta en la fase de requisitos, se priorizarán aspectos de seguridad, tales como:

1. El nivel de confianza requerido por la aplicación.
2. Los requisitos de autenticación.
3. Las especificaciones para el suministro de los accesos a los usuarios.
4. La necesidad de establecer usuarios privilegiados y técnicos de mantenimiento.
5. Notificación hacia los usuarios sobre sus responsabilidades y deberes.
6. Las necesidades de protección de los activos involucrados (análisis de riesgos), para garantizar la disponibilidad, confidencialidad e integridad.
7. Registro de las transacciones de los usuarios.
8. Las actividades que requieren supervisión y monitoreo, y de no repudio.
9. Los requisitos exigidos por otros controles de seguridad (interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos).
10. Asegurar que los requisitos establecidos se encuentren implementados a cabalidad durante las pruebas realizadas sobre los desarrollos del software.

11. Velar porque se apliquen los estándares de desarrollo definidos por la DSI.
12. Los desarrollos de sistemas de información contratados para ser realizados por terceros, docentes y administrativos deben cumplir con todos los lineamientos o estándares de desarrollo definidos por de la DSI y deberán suministrar, entre otras que requiera la Universidad, la documentación relacionada con:
    a. Manual del usuario que describa los procedimientos de operación.
    b. Manual técnico que describa su estructura interna, programas, catálogos y archivos, bases de datos, tablas.
    c. Código fuente.

8.15.1.2 Aseguramiento de los servicios de aplicación en las redes públicas.

Para la Universidad los servicios de aplicación son el medio con el que la Universidad automatiza ciertos procesos de comunicación, tramitación, entre otros, y los convierte en servicios para los grupos de interés.

La DSI velará porque la información involucrada en los servicios de las aplicaciones, a cargo de esta unidad, que pasan sobre redes públicas esté protegida de actividades fraudulentas, divulgación y modificaciones no autorizadas, para ello implementará mecanismos de control, tales como:

1. Encriptar la comunicación.
2. Definir el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte (por medio de autenticación) y si es necesario el uso de múltiples mecanismos de autenticación.
3. Determinar la necesidad de implementar mecanismos para la prevención de envío de información no permitida en redes públicas.
4. Establecer los procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales clave.
5. Asegurar que los involucrados estén completamente informados de sus autorizaciones para suministro o uso del servicio.
6. Definir el nivel de confianza requerido en la integridad de los documentos clave.
7. Establecer los requisitos de protección de cualquier información confidencial.
8. Definir la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibos.
9. Definir el grado de verificación apropiado de la información de pago suministrada por un cliente.
10. Seleccionar la forma de arreglo de pago más apropiado para protegerse contra fraudes.
11. Definir la responsabilidad civil asociada con cualquier transacción fraudulenta.
12. Determinar la necesidad de implementar sistemas de protección para envíos involuntarios de archivos.
13. Aplicar mecanismos de chequeo para verificar la integridad del software, firmware, e información.

14. Proteger los servicios asociados a transacciones electrónicas para evitar transmisión incompleta, alteración o divulgación no autorizada o enrutamiento errado.
15. Certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.
16. Evitar la pérdida o duplicación de información de la transacción.

8.15.1.3 Transacciones en línea

Las DSI aplicará controles, en los desarrollos a su cargo, para garantizar la protección de las transacciones entre aplicaciones y evitar:

1. Transacciones incompletas.
2. Mensajes no autorizados.
3. Alteración de los datos.
4. Divulgación de la información.
5. Duplicación de mensajes o reproducción no autorizada.
6. Afectar o comprometer la confidencialidad de las comunicaciones, mediante el uso de protocolos de comunicación seguros.

8.15.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

La Universidad garantiza que los protocolos de seguridad de la información se diseñan e implementan dentro del ciclo de vida del desarrollo de los sistemas de la información que son de misión crítica y están a cargo de la DSI.

8.15.2.1 Desarrollo seguro

La DSI aplica reglas para el desarrollo de software y de sistemas seguros, a los desarrollos que están a su cargo y que son considerados de misión crítica, entre ellas:

1. Define la seguridad del ambiente de desarrollo.
2. Orienta la seguridad en el ciclo de vida de desarrollo del software:
    a. Definiendo la seguridad en la metodología de desarrollo de software.
    b. Estableciendo las directrices de codificación seguras para cada lenguaje de programación usado.
3. Define la gestión de las distintas versiones de software.
4. Define los requisitos de seguridad en la fase diseño.
5. Define los puntos de chequeo de seguridad dentro de los hitos del proyecto.
6. Establece el conocimiento requerido sobre seguridad de la aplicación
7. Define la gestión de las vulnerabilidades de lo desarrollo: evitar, encontrar y resolver las vulnerabilidades.
8. Garantiza que todo el software desarrollado internamente cuenta con el nivel de soporte requerido.

9. Define la separación de los ambientes de desarrollo, pruebas y producción.
10. Obtiene aprobación de los propietarios de los sistemas de información en el desarrollo de nuevos sistemas o implementación de cambios o nuevas funcionalidades en los sistemas existentes.
11. Garantiza que las aplicaciones y desarrollos se diseñen y construyan en versiones vigentes y estables emitidas por el fabricante respecto a las herramientas, componentes, lenguajes de programación.
12. Establece la metodología para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
13. Almacena las copias de seguridad del código fuente de manera segura previendo riesgos asociados a pérdida de disponibilidad, confidencialidad o integridad.
14. Aplica el procedimiento de control de cambios a las modificaciones para el software, aplicaciones y sistemas de información a cargo.
15. verifica que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

A nivel de desarrolladores que forman parte del equipo de la DSI, tendrán en cuenta aspectos a cumplir, tales como:

1. Aplicar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los sistemas de información, pasando desde el diseño hasta la puesta en marcha.
2. Construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
3. Asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos, caracteres de alteración de rutas.
4. Suministran opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
5. Asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como parámetros adicionales de verificación.
6. Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos.
7. Garantizar que no se divulgue información confidencial en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
8. Remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
9. Prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

10. Remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
11. Evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
12. Certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
13. Desarrollar los controles necesarios para la transferencia de archivos, como: exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos, asegurar que dichos archivos sólo tengan privilegios de lectura.
14. Proteger el código fuente de las aplicaciones construidas, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
15. Asegurar que no se permita que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

8.15.2.2 Control de cambios de los sistemas de información

Cualquier tipo de cambio solicitado sobre los sistemas de información a cargo de la DSI seguirá los lineamientos establecidos en el procedimiento para mantenimiento de software y procesamiento de datos.

Durante el procedimiento de cambios, los desarrolladores realizarán acciones que les permitan:

1. Llevar un registro de los niveles de autorización acordados.
2. Asegurar que los cambios se presenten a los usuarios autorizados.
3. Revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios.
4. Identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección.
5. Identificar y verificar el código crítico de seguridad para minimizar la posibilidad de debilidades de seguridad conocidas.
6. Obtener aprobación formal para propuestas detalladas antes de que el trabajo comience.
7. Revisar Asegurar que los usuarios autorizados acepten los cambios antes de la implementación.
8. Mantener las evidencias documentales que soportan la trazabilidad de los cambios implementados, de acuerdo con las tablas de retención documental.
9. Mantener un control de versiones para todas las actualizaciones de software.
10. Mantener un rastro de auditoría de todas las solicitudes de cambio.
11. Asegurar que la documentación de operación y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados.
12. Asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados.

8.15.2.3 Revisión técnica de aplicaciones después de cambios de las plataformas operativas

Después de una actualización o cambios en la plataforma de operación la DSI revisará y probará las aplicaciones para garantizar que los cambios no afecten a su operatividad, para ello:

1. Revisará los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones.
2. Asegurará que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación.
3. Garantizará que se realicen los cambios apropiados en los planes de continuidad del negocio.

8.15.2.4 Restricciones a los cambios en los paquetes de software

LA DSI limitará los cambios en los paquetes software a su cargo, como medida de buena práctica para delimitar o minimizar la posibilidad de generar incidentes, por tanto, evitará aplicar cambios innecesarios y llevará acabo aquellos considerados necesarios, para ello revisará los siguientes criterios previo al ejercicio de planeación o implementación de los cambios:

1. Definir el riesgo de comprometer los procesos de integridad y controles existentes comparándolos con los beneficios de la actualización a realizar.
2. Obtener la aprobación del propietario del software.
3. Determinar si se puede evitar la actualización con versiones estables o estándares del software por parte del proveedor o vendedor.
4. Evaluar el impacto, si la Universidad llega a ser responsable del mantenimiento futuro del software como resultado de los cambios.
5. Establecer la compatibilidad con otro software en uso.

8.15.2.5 Principios de la ingeniería de Sistemas Seguros

La DSI definirá lineamientos para ingeniería segura de sistemas de información, tanto para el desarrollo de nuevos sistemas como para el mantenimiento de los sistemas existentes; también establecerá los estándares mínimos de seguridad que se deben cumplir.

8.15.2.6 Ambiente de desarrollo seguro

La DSI es la dependencia de la Universidad encargada de gestionar y proteger adecuadamente los ambientes de desarrollo, para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas, estableciendo controles de seguridad sobre los procesos o personas. Para ello requiere:

1. Determinar el carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir.
2. Definir los requisitos externos e internos aplicables, (reglamentaciones o políticas).
3. Definir los controles de seguridad para cada tipo de dato.
4. Establecer la confiabilidad del personal que trabaja en el ambiente.

5. Definir el grado de contratación externa asociado con el desarrollo del sistema, en caso de requerirse.
6. Definir la necesidad de separación entre diferentes ambientes de desarrollo
7. Definir el control de acceso al ambiente de desarrollo
8. Establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados.
9. Definir las necesidades de respaldo de información y si las copias de respaldo se almacenan en lugares seguros fuera del sitio.
10. Definir el control sobre el movimiento de datos desde y hacia el ambiente.

8.15.2.7 Desarrollo subcontratado

La Universidad por medio de la UAA contratante, con el asesoramiento y apoyo de la DSI y unidades que considere conveniente, supervisará y hará seguimiento a las actividades de desarrollo de sistemas contratados externamente, teniendo en cuenta los siguientes aspectos:

1. Definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente.
2. Establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.
3. Supervisar el cumplimiento de los requisitos de seguridad
4. Definir el suministro del modelo de amenaza aprobado, al desarrollador externo
5. Realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables.
6. Evidenciar que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad.
7. Evidenciar que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega.
8. Evidenciar de que se han hecho pruebas pertinentes para proteger contra la presencia de vulnerabilidades conocidas.
9. Definir los certificados de depósito de títulos en garantía.
10. Velar porque se incluyan en las minutas de los contratos los controles y auditorias requeridos por la Universidad.
11. Establecer que la Universidad es responsable de la conformidad con las leyes aplicables y con la verificación de la eficiencia del control.
12. Todo lo anterior debe ser plasmado en acuerdos firmados y consensuados con el proveedor

En el caso de compras de aplicaciones a terceros las UAA establecerán controles de seguridad, como:

1. Procesos de compras formales que incluyan periodos de prueba y validación del producto
2. Aplicar criterios de evaluación de riesgos para tomar medidas de control adicionales si el producto no satisface totalmente las necesidades de seguridad
3. A la hora de integrar un software en aplicaciones o sistemas propios se considerará si es necesario configurar las aplicaciones, sistemas y Software a implantar en relación a la

seguridad, elaborando consecuentemente los procedimientos y asegurándose de que sean implementados

4. Definir protocolos de homologación y aceptación de productos de forma que se incluyan siempre criterios de seguridad de la información
5. Aplicar los criterios de aceptación de productos en actualizaciones de Software y en nuevas funcionalidades de productos en cuanto a criterios de seguridad.
6. Velar porque las nuevas funcionalidades, a pesar de que ser importantes y útiles, no deben vulnerar la seguridad de los sistemas actuales para que sea aceptable.

8.15.2.8 Pruebas de seguridad y aceptación del sistema

Durante los desarrollos a cargo de la DSI se llevarán a cabo:

1. Pruebas de funcionalidad de la seguridad en los sistemas antes de pasar a producción los desarrollos.
2. Verificación de que los procesos de detección de incidentes son probados periódicamente.
3. Revisión de las pruebas y criterios de aceptación, establecidos previamente, para los sistemas de información nuevos, actualizaciones y nuevas versiones.

8.15.3 DATOS DE PRUEBA

La DSI garantizará la aplicación de controles de protección sobre datos utilizados para las pruebas de los desarrollos a su cargo

8.15.3.1 Protección De Datos De Prueba

Para la protección de los datos de prueba, la DSI garantizará:

1. Qué los procedimientos de control de acceso, que se aplican a los ambientes de producción, se aplicarán también a los ambientes de pruebas y en los casos en que no se puedan aplicar los mismos controles de seguridad se deberán establecer acuerdos de confidencialidad.
2. Que la información de producción se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas.
3. Que se realice una adecuada disposición final de la información de los ambientes de pruebas, una vez éstas han concluido las mismas.
4. Mecanismos de registro sobre el copiado de la información de producción a pruebas.
5. Que la información entregada a los desarrolladores para realizar sus pruebas no revelará información confidencial de los ambientes de producción.

8.16 POLÍTICA RELACIÓN CON PROVEEDORES

La Universidad por medio de sus UAA y los responsables de los activos de información garantizará, mediante el cumplimiento de la presente política, las condiciones de seguridad necesarias, en los

eventos en que, una empresa, personal externo o proveedor de servicio a la universidad, requiera tener acceso a los sistemas de información o a los recursos que manejan activos de información, realizando paralelamente supervisión del cumplimiento de dichas condiciones.

Los funcionarios responsables de la realización o firma de contratos o convenios con proveedores, se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información adoptadas por la Universidad.

Los contratos, en los casos que aplique, incluirán las clausulas o un documento adicional, en los cuales se evidencien los Acuerdos de Confidencialidad o Acuerdos de Intercambio de Información y la socialización o comunicación de las normas y procedimientos institucionales relacionados con la seguridad de la información que apliquen al proveedor, teniendo en cuenta a su vez los lineamientos establecidos en la política de seguridad de las comunicaciones.

8.16.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES

8.16.1.1 Responsabilidades para las relaciones con los proveedores.

Los responsables de activos de información de la Universidad garantizarán la protección de los activos institucionales a los que tengan acceso los proveedores, para ello se requiere:

1. Determinar los riesgos de seguridad de información a los cuales estarán expuestos los activos de información por la subcontratación o cesión de datos a terceros y analiza las posibles amenazas y el impacto que tendrían su pérdida de confidencialidad, integridad o disponibilidad de conformidad con los instrumentos dispuestos por la Universidad.
2. Establecer los mecanismos para mitigar los riesgos asociados por el acceso de los proveedores o personal externo.
3. En todos los contratos o acuerdos con proveedores, que implique un intercambio, uso o procesamiento de información, o uso de activos de información, se deben realizar acuerdos de confidencialidad sobre el manejo de la información, así como también cuando existan terceros autorizados por la Universidad que sean necesarios para cumplimiento de las obligaciones del contratista.
4. Dentro del contrato o acuerdo se debe definir claramente la clasificación de la información que se va a intercambiar por las partes de acuerdo a la clasificación institucional.
5. Al suscribir los acuerdos de confidencialidad se deben describir claramente los activos y clasificación de la información a los que tendrán acceso los proveedores, al igual que todos los requisitos de seguridad de la información acordados con estos, incluyendo las obligaciones del contratista al momento de la finalización o terminación del contrato, en relación con el manejo de la información conocida, tales como:

   a. La devolución de los activos de información.
   b. La eliminación o destrucción de datos.
   c. La cancelación y revocación de los accesos.
6. En los contratos o acuerdos con los proveedores o contratistas se incluirá como una causal de terminación del acuerdo o contrato de servicios, el no cumplimiento de las políticas de seguridad y privacidad de la información definidas por la Universidad.
7. Aplicar la política de control de acceso sobre los activos a los cuales accederá el proveedor.
8. Monitorean el cumplimiento de los controles establecidos en los acuerdos de prestación de servicio, por parte de los proveedores.
9. Establecen en los estudios previos, los requerimientos técnicos mínimos para la selección que contemplen la experiencia y reputación del proveedor o terceros, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad, tratamiento de datos personales y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

Cuando un proveedor, contratista o terceros requieren acceder a los sistemas de información o infraestructura tecnológica a cargo de la DSI, se deberá tener en cuenta lo siguiente:

1. Los proveedores que prestan servicios de soporte, mantenimientos o consultoría sobre sistemas de información e infraestructura tecnológica que se encuentren bajo supervisión de la DSI, no podrán tener acceso a los ambientes de producción.
2. Los proveedores que prestan servicios a las diferentes áreas de la Institución y que requieran acceder, a través de una cuenta institucional, a los servicios y recursos informáticos de la Universidad en aras de cumplir a cabalidad con las obligaciones del contrato, solo podrían contar con dicho acceso si cumplen en su totalidad con los siguientes requisitos:
   a. El funcionario responsable de la supervisión del contrato enviará solicitud justificada y aprobada por la unidad responsable de la información del sistema de información a la DSI, identificando el periodo de tiempo (fecha inicial y final) por el cual se requiere dar acceso al proveedor.
   b. El proveedor deberá tener suscrito un contrato vigente de prestación de servicios por medio del cual se regule los deberes de confidencialidad y manejo de la información o en su defecto de no tener contrato, deberá suscribir acuerdo de confidencialidad.
   c. Las DSI revisará la solicitud y podrá aprobarla o rechazarla de conformidad con el cumplimiento de las políticas de seguridad.

8.16.1.2 Requisitos en los acuerdos con proveedores.

La UAA en el momento de establecer los acuerdos de niveles de servicios definirá las condiciones de seguridad de la información dejándolas documentadas en los contratos de forma explícita o en un apartado o anexo suscrito por las partes.

A continuación, se indican los requisitos mínimos de seguridad que las UAA pueden exigir al proveedor, sin perjuicio de los demás requisitos que se identifiquen según cada caso concreto:

1. Solicitar al proveedor la designación de un responsable de seguridad, quien será el interlocutor ante cualquier tema de seguridad y de aplicar los controles pactados entre las partes.
2. Establecer que el proveedor informe sobre cualquier cambio de personal dedicado a la prestación de servicios dentro del acuerdo firmado y que en caso de retiro o rotación del personal se solicite la revocación de los permisos de acceso tanto a las instalaciones como a los sistemas de información.
3. Definir cómo y cuándo se realizarán las comunicaciones con el proveedor
4. Confirmar que el proveedor cumple los requisitos legales sobre la protección de datos etc. Obtenga su compromiso por escrito
5. Establecer por escrito una cláusula en la cual el proveedor se comprometa a hacer uso correcto de los activos para la finalidad prevista y que aplicará medidas de control para evitar el daño o revelación de la información y los accesos no autorizados.
6. Establecer si existe la necesidad de aplicar auditorías de seguridad al personal o a las instalaciones.
7. Establecer clausulas específicas, en caso de necesidad, para que el proveedor mantenga procesos de seguridad, tales como: contratación, devolución o destrucción de la información a la finalización del acuerdo, formación en seguridad de la información, control de cambios, tratamiento de incidencias u no conformidades, escalado en la resolución de incidencias, actualización de software y programas de seguridad (antivirus firewall etc.), emergencia y de recuperación de desastres, otros.

8.16.2 GESTIÓN DE LA ENTREGA DEL SERVICIO POR PROVEEDORES

La Universidad por medio de la UAA contratante velará por mantener los niveles de seguridad de la información y de prestación de los servicios de sus proveedores en concordancia con los acuerdos establecidos, al igual velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

8.16.2.1 Seguimiento y revisión de los servicios de proveedores

La revisión y seguimiento de los servicios de los proveedores será realizada por la UAA contratante teniendo en cuenta la reglamentación institucional relativa a la supervisión de los contratos.

8.16.2.2 Gestión de cambios en los servicios de los proveedores

En el caso de que la UAA contratante requiera aplicar cambios a los servicios prestados por los proveedores, deberían:

1. Aplicar un análisis de riesgos al nuevo escenario.
2. Evaluar la necesidad de modificar o ampliar los acuerdos de prestación de servicios para cubrir las nuevas necesidades de seguridad si así se estima oportuno.

8.17 POLÍTICA GESTIÓN DE INCIDENTES Y MEJORAS DE SEGURIDAD DE LA INFORMACIÓN.

La Universidad Industrial de Santander gestiona de manera ágil y eficiente los incidentes de seguridad de la información, para ello las UAA responsables de sus activos de información críticos y el Equipo de Gestión de Incidentes de Seguridad **(EGIS**) establecerán los mecanismos de protección y mitigación relacionados con incidentes de seguridad que se puedan presentar, incluida la comunicación sobre estos eventos.

DEFINICIONES

- **EVENTO EN LA SEGURIDAD DE LA INFORMACION:** Cualquier ocurrencia identificada en un sistema de información, servicio o estado de la red que indica 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 INFORMACION:** 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)

8.17.1 Responsabilidades y procedimientos

1. El Equipo de Gestión de Incidentes de Seguridad definirá y comunicará los procedimientos para la gestión de los incidentes seguridad de información digital dentro de la Universidad, entre los cuales se requieren:
    a. Procedimientos para la planificación y preparación de respuestas a incidentes.
    b. Procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información.
    c. Procedimientos para el registro de las actividades de gestión de incidentes.

d. Procedimiento clasificación de eventos y debilidades de seguridad de la información para la toma de decisiones.
e. Procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas.
f. Procedimiento para la estrategia de comunicación a utilizar para reportar a las personas o entidades que se requieran en caso de escalar el incidente.

2. Cada UAA define un responsable o responsables para la gestión de los incidentes que se puedan presentar en sus activos de información críticos.
3. El responsable o responsables de incidentes de seguridad deberán investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, proporcionando las soluciones y aplicando los correctivos para mitigar una nueva ocurrencia.
4. Es deber de los funcionarios de la Universidad, estudiantes, colaboradores, proveedores o terceros, reportar de forma inmediata eventos, incidentes o debilidades de seguridad de información detectadas en la infraestructura institucional.
5. Los usuarios que realicen actividades que impliquen la vulneración de la seguridad de la infraestructura tecnológica o servicios informáticos, estarán incumplimiento con las políticas de seguridad y estas actividades producirán las consecuencias disciplinarias a que haya lugar.
6. Las UAA establecerán un plan de capacitación, en corresponsabilidad con DGTH, para las personas que se ocupan de los incidentes de la seguridad de la información.
7. El Equipo de Gestión de Incidentes de Seguridad (EGIS) dispondrá de un punto de contacto para el reporte de incidentes de seguridad detectados.

8.17.2 Reporte de eventos y vulnerabilidades de seguridad de la información.

Sobre el reporte de eventos y debilidades las UAA deberán:

1. Ratificar que es responsabilidad de cada uno de los funcionarios de la Universidad, estudiantes, proveedores o terceros, reportar de forma inmediata los eventos, incidentes o vulnerabilidades de seguridad de información detectadas.
2. Establecer el canal o canales de comunicación que pueden utilizar los usuarios tanto internos como externos, para el reporte de todos los eventos o vulnerabilidades de seguridad. Estos canales, deben estar establecidos con los responsables de la gestión de los incidentes.
3. Informar y concientizar a todos los usuarios sobre los mecanismos o canales de notificación existentes para el reporte de eventos o debilidades de seguridad de información.
4. Llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos, recolectando las evidencias necesarias lo más pronto posible después del reporte del incidente. Aplica para los activos de información crítica de la UAA.

Las actividades a realizar sobre este aparte serán ejecutadas dando cumplimiento a los procedimientos establecidos por la Universidad.

8.17.3 Evaluación y decisión sobre los eventos de seguridad de información.

Las UAA y el Equipo de Gestión de Incidentes de Seguridad (EGIS) dispondrán de la información necesaria para el análisis, evaluación y toma de decisiones sobre los incidentes de seguridad presentados.

Las actividades a realizar sobre este aparte serán ejecutadas dando cumplimiento a los procedimientos establecidos.

8.17.4 Respuesta a incidentes de seguridad de la información

1. Las UAA y el Equipo de Gestión de Incidentes de Seguridad (EGIS) establecerán los mecanismos de respuesta a los incidentes de seguridad de la información.
2. Las UAA evaluarán si dispone de la capacidad para resolver el incidente por si misma o necesita ayuda de Equipo de Gestión de Incidentes de Seguridad (EGIS) o terceros.

Las actividades a realizar sobre este aparte serán ejecutadas dando cumplimiento a los procedimientos establecidos

8.17.5 Gestión de conocimiento sobre los incidentes de seguridad de la información

La Universidad Industrial de Santander considera que los incidentes de seguridad de la información son fuente de información para estudio y solución de futuros incidentes e incluso para mejorar la seguridad de la información institucional, por ende, las UAA y el Equipo de Gestión de Incidentes de Seguridad (EGIS) analizarán la información recopilada y relacionada con el incidente de manera tal que se documente el aprendizaje adquirido.

Las actividades a realizar sobre este aparte serán ejecutadas dando cumplimiento a los procedimientos establecidos.

8.17.6 Recolección de evidencia

Las UAA y Equipo de Gestión de Incidentes de Seguridad definirán y aplicarán directrices para la identificación, recolección, adquisición y preservación de evidencias de información, que posteriormente podrían ser utilizadas para acciones legales, sanciones disciplinarias, análisis forense o esclarecer escenarios, etc.

Las actividades a realizar sobre este aparte serán ejecutadas dando cumplimiento a los procedimientos establecidos.

8.18 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DE LAS FUNCIONES INSTITUCIONALES

La Universidad Industrial de Santander por medio de las UAA gestiona la continuidad de las funciones institucionales en relación a la seguridad de la información, estableciendo medidas que le permitan dar continuidad a las operaciones tecnológicas de sus procesos, tales como: a) analizar las necesidades y riesgos a los cuales está expuesta la UAA ante posibles desastres naturales o crisis (inundaciones, actos vandálicos, incendios y otras amenazas similares); b) minimizar los daños y facilitar el restablecimiento de sus operaciones; c) planificar las diferentes respuestas a los incidentes y lograr recuperarse ante desastres.

Para ello la UAA desarrollará los siguientes lineamientos:

8.18.1 Gestión de la continuidad de las funciones

8.18.1.1 Planificación de la continuidad de las funciones

1. La UAA con activos de información crítica, velará por establecer un BCP (Bussines Continuity Plan) o un DRP (Disaster Recovery Plan) que le permita garantizar la continuidad de sus operaciones ante desastres de seguridad de información anticipándose a riegos, respuestas o tratamiento a incidentes de esta índole.
2. La UAA Integrará en los planes de continuidad o planes de recuperación, las condiciones adecuadas de seguridad de la información en situaciones de crisis o ante desastres.
3. Se deberá disponer de planes de respuesta a incidentes y recuperación de incidentes por parte de las UAA.
4. En caso de que la UAA no cuenten con un plan de continuidad formal, ante una situación de parada de los distintos servicios (energía, comunicaciones, red, colapso de infraestructuras etc.), como alternativa, deberá:
    a. Llevar a cabo un análisis de impacto en las operaciones relacionadas con los aspectos de seguridad de la información.
    b. Evaluar y asumir el riesgo residual por la ausencia de los planes.

8.18.1.2 Implementación de la continuidad de las funciones

1. La UAA establecerá una estructura de gestión adecuada (funciones, responsabilidades, niveles de competencia) para prepararse, mitigar y responder a un evento contingente.
2. La UAA definirá el personal que dará respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información.

3. La UAA deberá definir, documentar y aprobar los planes y procedimientos de respuesta y recuperación, especificando en detalle como gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados en el ítem anterior.

8.18.1.3 Verificar, revisar y evaluar la continuidad de las funciones

1. La UAA realizará pruebas de funcionalidad de los procesos, procedimientos y controles aplicados a la continuidad del negocio de las operaciones y a los planes de recuperación de desastres en relación a la seguridad de la información, para asegurar que sean eficaces con los objetivos propuestos.
2. La UAA definirá la periodicidad de las pruebas de continuidad del negocio y de los planes de recuperación ante desastres.
3. Las UAA verificarán el desempeño del personal validando que las tareas de recuperación se lleven a cabo totalmente con base en las responsabilidades asignadas.

8.18.2 ASPECTOS DE LA REDUNDANCIA EN RELACIÓN A LA CONTINUIDAD DE LAS FUNCIONES

La Universidad aplicará mecanismos de redundancia que velarán por garantizar la disponibilidad de las instalaciones de procesamiento de información que ejecutan procesos críticos.

8.18.2.1 Disponibilidad de las instalaciones de procesamiento de información

1. Las UAA velarán por establecer medidas que le permitan dar continuidad a las operaciones tecnológicas en sus centros de datos (principal y alterno), o mantener la disponibilidad de componentes redundantes en caso de contar con solo uno de ellos.
2. Las UAA establecerán las directrices para definir y seleccionar qué elementos deben ser redundantes.
3. Las UAA garantizan que se apliquen las pruebas para asegurar que un componente redundante funcionará de la forma prevista durante una emergencia o falla.

8.18.3 RESPALDO DE INFORMACIÓN EN RELACIÓN A LA CONTINUIDAD DE LAS FUNCIONES

La Universidad a través de la DSI, define lineamientos para el respaldo de las aplicaciones institucionales y plataformas tecnológicas de misión crítica, en pro de la continuidad del negocio.

8.18.3.1 Respaldo de la información de las aplicaciones y datos institucionales

1. La realización de las copias de seguridad se realizará teniendo en cuenta las directrices expuestas en la guía para le realización de backup y en los formatos de control y entrega de backup definidos por la DSI.
2. La DSI es la dependencia de la Universidad encargada de realizar el respaldo diario y semanal de las aplicaciones institucionales en los servidores bajo la custodia y administración directa de la DSI.
3. El respaldo de la información de las bases de datos de producción bajo la custodia y administración directa de la DSI, se realiza todos los días de la semana en una hora definida por la DSI.
4. Las UAA que posean aplicaciones y datos bajo su administración serán responsables de definir y realizar los procesos de respaldo que consideren necesarios.

8.18.3.2 Respaldo de la información almacenada en los equipos de usuario final

1. El usuario es el responsable de realizar la copia de respaldo de la información resultado de las funciones de su cargo, alojada en el equipo de cómputo asignado y utilizando los recursos con que cuenta la Universidad en la actualidad, ya sea almacenamiento en la nube o en dispositivos hardware local de la UAA.
2. Las UAA podrán definir la necesidad de implementar mecanismos (automatizado o semiautomatizado) que permitan la realización de copias de respaldos de la información de los funcionarios a su cargo. Dicha implementación y gestión quedará a cargo de la UAA implementadora.
3. Al realizar copias de respaldo de la información las UAA tendrán en cuenta los lineamientos definidos en la Política sobre Almacenamiento.

8.18.3.3 Respaldo de la Información alojada en la nube

1. Las UAA podrán almacenar la documentación generada por sus actividades y labores, en los espacios de almacenamiento en la nube aprobados por la Universidad y velarán por mantener copias de seguridad de la misma en caso de algún incidente informático.
2. El servicio de almacenamiento en la nube es ofrecido por un proveedor externo contratado por la universidad, respecto del cual, la DSI se encargará de velar y monitorear la calidad de la prestación del servicio.
3. La información alojada en las cuentas de correo institucional, que sean desactivadas, se conservará de acuerdo al periodo establecido por el proveedor contratado y a las disposiciones establecidas en la política del uso del correo electrónico institucional.

8.19 POLÍTICAS DE CUMPLIMIENTO LEGAL

Las directrices relacionadas a continuación, están encaminadas a garantizar el cumplimiento de las políticas, leyes, normas y reglamentación aplicable a la Universidad y a sus funcionarios, enfocándose principalmente en lo que se refiere a seguridad de la información digital.

8.19.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES

La Universidad, a través de los funcionarios de las diferentes UAA, velará por la identificación, documentación y cumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información digital y con los requisitos de seguridad, emanados por la normatividad del estado colombiano y por la misma universidad

8.19.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

1. La Universidad definirá un mecanismo para identificar, documentar y mantener actualizada la relación de los requisitos legales y reglamentos estatutarios vigentes que en materia de seguridad de la información digital le apliquen a la Universidad.
2. La Universidad definirá el responsable de identificar y actualizar los requisitos legales, reglamentarios o estatutarios vigentes que le apliquen a la Universidad.
3. La Universidad dará a conocer el cumplimiento y estado normativo a aplicar y asignará los recursos para la implementación de controles de seguridad sobre la información digital.

8.19.1.2 Derechos de propiedad intelectual y uso de software legal

1. La Universidad cuenta con el reglamento de propiedad intelectual, guías, formatos y procedimientos que deben acoger y cumplir los miembros de la comunidad universitaria, para la protección de la propiedad intelectual resultante de investigaciones institucionales, participaciones en actividades de extensión y cualquier otra que sea susceptible de protección, respecto de las cuales, la Universidad sea el titular, total o parcial.
2. Para el uso de software y licencias los funcionarios de las UAA acatarán la política institucional "Política Uso de Software y Licencias" (ver política de gestión de activos)
3. Las UAA mantendrán un inventario respecto del software y sistemas de información que se encuentren permitidos en las estaciones de trabajo, equipos de cómputo y móviles a cargo de los funcionarios de la UAA.
4. Las UAA verificaran periódicamente que el software instalado corresponda únicamente al permitido. Este inventario debe contener la evidencia de la propiedad de las licencias.
5. Las UAA que celebren contratos con proveedores, deberán incluir una cláusula donde el proveedor garantiza que tiene las patentes o derechos de propiedad sobre el bien o servicio adquirido o contratado por la Entidad, cuando aplique.
6. Las UAA determinarán la necesidad de aplicar cláusulas de indemnidad con el propósito de asegurar que el proveedor defienda a la Universidad en sus derechos ante reclamos sobre infracciones sobre patentes (hardware) o derechos de autor (software). En el supuesto que se compruebe una infracción, deberá asegurarse una solución que no afecte los servicios de

la Universidad, ni comprometa la responsabilidad de la Universidad respecto de los eventuales daños y perjuicios causados.

7. Las UAA que celebren contratos con proveedores de desarrollo deben contemplar todo lo relacionado con los derechos de explotación y propiedad de los desarrollos, enumerando los derechos de explotación cedidos o de propiedad de la UIS, tales como: reproducción, distribución, comunicación pública y transformación sobre el resultado del desarrollo a favor de la Universidad, de conformidad con el Reglamento de Propiedad Intelectual y las leyes que regulan la materia.
8. Las UAA incluirán en los contratos una cláusula sobre la reserva de los derechos de propiedad intelectual, en la que se indique de forma expresa la reserva de todos los derechos existentes sobre el sitio web institucional.
9. Para las aplicaciones Web de la Universidad que son ejecutadas de forma remota por los usuarios, no siendo necesaria la descarga o instalación de software alguno en su equipo, se debe aclarar en la licencia de uso una protección tanto a la aplicación, como a los contenidos que son ejecutados a través de la misma.
10. Las UAA sensibilizarán a los funcionarios, temporales y contratistas en la instalación y uso de software legal para proteger los derechos de propiedad intelectual, e incluso sensibilizarán sobre las acciones disciplinarias en caso de incumplir la normativa.
11. Las UAA deberán asegurar que poseen los derechos de uso o el licenciamiento apropiado para todo el software que lo requiera o alternativamente se permite utilizar software de libre distribución y uso.
12. Para el uso de licencias limitadas por tiempo o por tipo de uso, el responsable del activo de información deberá garantizar que se cumple lo establecido por este tipo de licenciamiento.
13. Los profesores, administrativos, estudiantes y terceros deben cumplir con la normativa de derechos de autor y acuerdos de licenciamiento de software. La instalación de copias de un software en diferentes equipos sólo se podrá realizar si el tipo de licenciamiento lo permite.

8.19.1.3 Protección de los registros

La Universidad protege los registros de su información, de pérdida, destrucción y falsificación en concordancia con la reglamentación interna que aplique. Para ello:

1. Las UAA mantendrán un inventario actualizado de los registros de activos de información producido en razón de sus funciones de competencia, según lo establecido en las tablas de retención documental.
2. La Universidad definirá y publicará las directrices sobre la organización, retención, almacenamiento, tratamiento y eliminación de los registros y la información de conformidad con los instrumentos archivísticos.
3. Las UAA en coordinación con la Dirección de Certificación y Gestión Documental y la División de Servicios de Información definirán los registros y soporte documentales (físico o electrónico) que serán protegidos según la criticidad de sus operaciones teniendo en cuenta los instrumentos archivísticos.

8.19.1.4 Protección de los datos y privacidad de la información personal

La Universidad por medio de los funcionarios y contratistas de las respectivas UAA asegura la protección y privacidad de la información personal de los miembros de la comunidad universitaria o personal externo, tal como se requiere en la legislación vigente, la Reglamentación Institucional y, si fuese aplicable, las cláusulas contractuales. Para ello:

1. La Universidad por medio del manual de procedimiento administrativo para el tratamiento de los datos personales, establece las directrices que las UAA y funcionarios acatarán sobre el cumplimiento de la ley para la privacidad de los datos personales.
2. La Universidad mantendrá publicada en el sitio web institucional la Política de Tratamiento de Datos Personales aprobada.
3. La Universidad capacitará y sensibilizará en los lineamientos de la ley de protección de datos personales al personal de la Universidad, y coordinará la divulgación, por medio de las UAA, de estos lineamientos a los proveedores y terceras partes interesadas.

8.19.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

La Universidad por medio de la Dirección de Control Interno y Evaluación de Gestión validará que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos Institucionales.

8.19.2.1 Revisión independiente de la seguridad de la información

1. La Dirección de Control Interno y Evaluación de Gestión, como Unidad encargada del control y seguimiento de los procesos institucionales podrá establecer planes de auditorías sobre seguridad y privacidad de la información en las UAA que lo ameriten
2. La Dirección de control interno y evaluación de gestión dará a conocer los resultados de las auditorías y establecerá las oportunidades de mejora o los cambios que se estimen necesarios relacionados con la seguridad de la información para la UAA intervenida.
3. La UAA que lo considere pertinente podrá optar por realizar auditorías relacionadas con la seguridad y privacidad de la información, por parte de personas o entidades externas con previo aval del Comité Institucional de Gestión y Desempeño, con el fin de aplicar mejoras en la implementación de los controles adoptados para la gestión de la seguridad de la información.
4. Los directores o jefes de las UAA deben apoyar las revisiones del cumplimiento de las políticas de seguridad de la información y atender cualquier requerimiento de seguridad que les sea realizado.

8.19.2.2 Cumplimiento de la política y las normas de seguridad

Las UAA garantizarán el cumplimiento de las políticas y estándares de seguridad aprobados por la Universidad, al interior de estas. Para ello:

1. Asegurarán que todos los procedimientos y requisitos de seguridad de información, dentro de su área de responsabilidad se lleven a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad.
2. Realizarán revisión periódica del cumplimiento de las políticas y normas de seguridad establecidas para los centros de datos y sistemas de información que apoyan los procesos de la unidad.
3. Revisarán regularmente los sistemas de información para asegurar el cumplimiento de las normas de seguridad de la información
4. En caso de incumplimiento se deberán determinar las causas, la evaluación de las medidas a tomar, la implementación de las acciones correctivas apropiadas, la revisión de la eficacia de las acciones correctivas, la identificación de las deficiencias y las debilidades del sistema.
5. Podrán solicitar asesoría a la División de Servicios de Información en los momentos que lo requieran, sobre el cumplimiento de los lineamientos técnicos relacionados con seguridad digital que sean de su competencia.
6. Mantendrán registros documentados de los resultados de las revisiones y de las acciones correctivas ejecutadas para poder realizar informes con los resultados.

8.19.2.3 Revisión del cumplimiento técnico

1. Las UAA revisarán periódicamente que los activos de información que estén bajo su responsabilidad directa permanezcan configurados correctamente de acuerdo a las reglas y políticas institucionales definidas, con fin de:
    a. Identificar actualizaciones necesarias que corrijan fallos de seguridad.
    b. Establecer medidas correctivas antes de que estos fallos puedan suponer una amenaza real.
    c. Planear la sostenibilidad y administración del activo durante su ciclo de vida.
2. Las UAA realizarán evaluaciones de seguridad técnica sobre los activos de información bajo su responsabilidad, con la supervisión de personal experto y autorizado, y apoyándose en herramientas automatizadas o con revisiones manuales realizadas por especialistas.
3. En los casos que le compete, la DSI emitirá el aval respectivo para la elección del perfil del experto (persona/entidad) externo, que realizará la(s) evaluación(es) técnicas en relación a la seguridad digital.
4. Las UAA dejarán evidencias de las pruebas realizadas, sus resultados y seguimiento para asegurar que las brechas de seguridad halladas se han solucionado.