PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

INSTITUCION UNIVESITARIA BELLAS ARTES Y CIERNCIAS DE BOLIVAR

Enero 2026

www.unibac.edu.co
info@unibac.edu.co
PBX. +605 6724603
Cra. 9 No. 39-12
Centro Histórico
Cartagena de Indias
Bolívar, Colombia
Síguenos como Unibac:

1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la institución universitaria bellas artes y ciencias de bolívar con respecto a la protección de los activos de información (los funcionarios, contratistas, estudiantes, terceros, información, procesos, las tecnologías de información incluido el hardware que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Para asegurar el direccionamiento estratégico de la institución, establece la compatibilidad de la política y de los objetivos de seguridad de la información, estos últimos correspondientes a:

- Mantener la confianza de los funcionarios, contratistas, estudiantes y terceros.
- Apoyar las iniciativas de innovación tecnológica.
- Cumplir con los principios de la función administrativa.
- Cumplir con los principios de seguridad de la información.
- Custodiar y Proteger los activos de información.
- Garantizar la continuidad del servicio frente a incidentes.
- Apoyar el proyecto "Generación U", garantizando la disponibilidad y calidad de los datos para la toma de decisiones estratégicas.
- Integrar tecnologías de vanguardia como Inteligencia Artificial (IA) y Machine Learning (ML) para la detección temprana de amenazas.
- Cumplir con la Ley 1581 de 2012 (Protección de Datos) y la Ley 1712 de 2014 (Transparencia).
- Custodiar y proteger la infraestructura crítica, incluyendo la nueva sede Unibac Matuna.

1.1 Alcance

Esta política aplica a todos los funcionarios, contratistas, estudiantes y terceros, extendiéndose al nuevo "Ecosistema Digital Unibac" que abarca infraestructura, usuarios, servicios y aplicaciones l.

A continuación, se establecen las políticas que soportan el plan de seguridad y privacidad de la información de la institución Universitaria Bellas artes y Ciencia de Bolívar.

a. La institución Universitaria Bellas Artes y ciencias de Bolívar protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.

b. La institución Universitaria Bellas Artes y ciencias de Bolívar protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

c. La institución Universitaria Bellas Artes y ciencias de Bolívar controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.

d. La institución Universitaria Bellas Artes y ciencias de Bolívar garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

e. La institución Universitaria Bellas Artes y ciencias de Bolívar protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

f. La Institución Universitaria Bellas Artes y ciencia de Bolívar garantiza el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

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

2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

2.1 Justificación

Para Unibac, la información es su principal activo estratégico. La transición a Universidad exige niveles superiores de integridad, disponibilidad y confidencialidad para soportar procesos de alta calidad académica y administrativa, minimizando riesgos de pérdida o accesos no autorizados.

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

a) Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

b) Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

c) Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

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

b) Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

c) No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

d) Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

A los efectos de una correcta interpretación del presente Plan, se realizan las siguientes definiciones:

- Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
- Sistema de Información: se refiere a un conjunto independiente de recursos de procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- Tecnología de la Información: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2 Roles y Responsabilidades

La implementación y seguimiento son responsabilidad del Comité de Seguridad de la Información, o quien haga sus veces, el cual debe sesionar anualmente para actualizar la política. Este comité está compuesto por:

a. Rectoría.

b. Vicerrectorías (Académica, Financiera, Administrativa).

c. Secretaría General.

d. Profesionales de Planeación, Gestión TIC, Comunicaciones, Archivo y Almacén.

Este comité deberá revisar y actualizar esta política anualmente presentando las propuestas a la alta dirección para su aprobación.

2.3 Cumplimiento

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, la Institución Universitaria Bellas Artes y ciencias de Bolívar se reserva el derecho de tomar las medidas correspondientes.

2.4 Comunicación

Mediante socialización a todos los funcionarios de la Institución Universitaria Bellas Artes y ciencias de Bolívar dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad www.unibac.edu.co.

2.5 Monitoreo

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario. .

3. DESCRIPCIÓN DE LAS POLÍTICAS

Generalidades

La Institución Universitaria Bellas Artes y Ciencias de Bolívar en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

De acuerdo a esta Política se divulgan los objetivos y alcances de seguridad de la información de la institución, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad en la CMV.

3.1 Gestión de Activos

Unibac mantendrá un inventario clasificado y valorado de activos de información física y digital. Se priorizará la protección de los sistemas core: SAU (Académico), SAFE (Financiero), PROYECTO E y ORBIS (Gestión Documental).

3.1.1 Política para la identificación, clasificación y control de activos de información.

La Institución Universitaria Bellas Artes y ciencias de Bolívar través del Comité de Seguridad de la Información realizará la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo a Gestión de TIC y a Gestión Documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

El facilitador del proceso de Gestión de Recursos Físicos con apoyo del técnico operativo de sistemas tiene la responsabilidad de mantener el inventario completo

y actualizado de los recursos de hardware y software de la entidad.

Pautas para tener en cuenta

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

- La información física y digital de la Institución debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad.

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

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

3.2 Control de Acceso

- Acceso a Redes: La red LAN de 10 Gbps segmentada por VLANs y los perímetros protegidos por Firewall contarán con controles estrictos de autenticación lógica.
- Gestión de Usuarios: Se establece un protocolo para la creación, bloqueo y eliminación oportuna de cuentas ante desvinculaciones o traslados de personal.
- Configuración: Las contraseñas deben seguir lineamientos de complejidad, cambio periódico y control histórico.

3.2.1 Política de acceso a redes y recursos de red

El técnico operativo de sistemas de la Institución Universitaria Bellas Artes y Ciencia de Bolívar, como responsable de las redes de datos y los recursos de red

de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Pautas para tener en cuenta

- El proceso Gestión de TIC debe asegurar que las redes inalámbricas de la institución cuenten con métodos de autenticación que evite accesos no autorizados.

- El proceso Gestión de TIC debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de la Institución Universitaria Bellas Artes y Ciencia de

Bolívar, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

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

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

3.2.2 Política de administración de acceso de usuarios

La Institución Universitaria Bellas Artes y ciencias de Bolívar establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Pautas para tener en cuenta

- El proceso Gestión de TIC, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la institución universitaria; dichos cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

- El proceso Gestión de TIC debe establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.
- El proceso Gestión de TIC debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.
- Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con el proceso Gestión de TIC las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

3.2.3 Política de control de acceso a sistemas de información y aplicativos

La Institución Universitaria Bellas Artes y ciencias de Bolívar como propietario de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

El proceso Gestión de TIC, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, vela porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Pautas para tener en cuenta

- Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.
- Los propietarios de los activos de información deben monitorear anualmente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.
- El proceso Gestión de TIC debe establecer un protocolo para la asignación de accesos a los sistemas y aplicativos de la Contraloría Municipal de Villavicencio.
- El proceso Gestión de TIC debe establecer el protocolo y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- El proceso Gestión de TIC debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
- Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

3.2.4 Políticas de seguridad física

La Institución Universitaria Bellas Artes y ciencias de Bolívar provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

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 considera áreas de acceso restringido.

Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones.

El proceso Gestión de TIC mantiene las normas, controles y registros de acceso a dichas áreas.

Pautas para tener en cuenta

- Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobadas por funcionarios que apoyan el proceso Gestión de TIC autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario.
- El proceso Gestión de TIC debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.
- El (la) Director (a) debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la institución Universitaria.
- El (la) Director (a) debe identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la institución.
- Los ingresos y egresos de personal a las instalaciones de la institución en horarios no laborales deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
- Los funcionarios deben portar el carné que los identifica como tales en un lugar visible; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible.

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

4. PRIVACIDAD Y CONFIDENCIALIDAD

4.1 Política de tratamiento y protección de datos personales

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, la Institución Universitaria Bellas Artes y ciencias de Bolívar a través del Comité de Seguridad de la Información, propende por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establece los términos, condiciones y finalidades para las cuales la Institución Universitaria Bellas Artes y ciencias de Bolívar, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la institución Universitaria exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Pautas para tener en cuenta

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

asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

- Las Unidades de gestión que procesan datos personales de beneficiarios, funcionarios, estudiantes, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
- Las Unidades de gestión que procesan datos personales de beneficiarios, funcionarios, estudiantes, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.
- Las Unidades de gestión que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.
- El comité de seguridad de la información debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, estudiantes, proveedores y demás terceros de la institución Universitaria Bellas Artes y Ciencia de Bolívar de los cuales reciba y administre información.
- El proceso Gestión de TIC debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, estudiantes, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.
- Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

4.2 Disponibilidad del servicio e información

La Institución Universitaria Bellas Artes y ciencias de Bolívar con el propósito de garantizar la disponibilidad de la información y mantener los servicios orientados con el objetivo de la entidad y los ofrecidos externamente, a decidido crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

Unibac garantiza la continuidad mediante:

- Copias de Seguridad: Backups automáticos de bases de datos y sistemas de misión crítica almacenados en sitios seguros.
- Pruebas de Restauración: Realización de simulacros periódicos para verificar que los datos sean legibles.
- Recuperación ante Desastres: Un plan que define el Tiempo Óptimo de Recuperación (RTO) para procesos críticos.

4.2.2 Política de continuidad, contingencia y recuperación de la información

La Institución Universitaria Bellas Artes y ciencias de Bolívar proporcionará los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

4.2.2.1 Copias de Seguridad

Toda información que pertenezca a la matriz de activos de información institucional o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Seguridad de la Información. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

Las dependencias de la Institución Universitaria Bellas Artes y ciencias de Bolívar debe realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin.

La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

Pautas para tener en cuenta

a. El Comité de Seguridad de la Información, debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

b. El Comité de Seguridad de la Información, debe liderar los temas relacionados con la continuidad de la entidad y la recuperación ante desastres.

c. El Comité de Seguridad de la Información debe realizar los análisis de impacto al entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

d. El Comité de Seguridad de la Información debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

e. El Comité de Seguridad de la Información, debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de entidad, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

5. Políticas de Seguridad

5.1 Formación y Concientización

Descripción: La formación y concientización son elementos clave en la estrategia de seguridad de Unibac. Este componente del plan se centra en el desarrollo de programas continuos de educación para todos los miembros de la comunidad académica y administrativa. El propósito es dotar a los usuarios con el conocimiento necesario para entender las políticas de seguridad, reconocer posibles amenazas y

adoptar prácticas seguras en el uso de la tecnología.

Objetivos:

- Concientización sobre Ciberseguridad: Proporcionar información regular sobre las últimas amenazas de seguridad cibernética y mejores prácticas para mitigar riesgos.
- Entrenamiento en Políticas de Seguridad: Garantizar que todos los usuarios comprendan y cumplan las políticas de seguridad establecidas por Unibac.
- Simulacros de Phishing: Realizar simulacros periódicos de phishing para sensibilizar a los usuarios sobre las posibles amenazas y mejorar su capacidad para reconocer intentos de ingeniería social.
- Uso Seguro de Recursos Digitales: Ofrecer orientación sobre el uso seguro de plataformas digitales, redes sociales y otros recursos en línea, enfocándose en la protección de datos personales.
- Manejo de Información Confidencial: Educar a los usuarios sobre la importancia de manejar información confidencial y proporcionar directrices claras sobre cómo almacenar, compartir y desechar adecuadamente la información.
- Uso de IA: Orientación sobre el manejo ético y seguro de herramientas de IA generativa.

Métodos de Implementación:

- Sesiones de Capacitación: Realizar sesiones periódicas de capacitación presencial y virtual.
- Materiales Didácticos: Desarrollar materiales educativos, como folletos, videos y correos electrónicos informativos.
- Simulacros Interactivos: Realizar simulacros interactivos para evaluar la preparación de los usuarios ante posibles amenazas.

Indicadores de Éxito:

- Participación Activa: Porcentaje de usuarios que participan en programas de formación y concientización.

- Reducción de Incidentes: Medir la disminución de incidentes de seguridad relacionados con acciones no seguras por parte de los usuarios

6. Procedimientos Operativos

6.1 Procedimientos Operativos

6.1.1.1 Monitoreo Continuo y Respuesta a Incidentes

Descripción: Los procedimientos operativos para el monitoreo continuo y la respuesta a incidentes son fundamentales para mantener un entorno seguro en Unibac. Estos procedimientos están diseñados para identificar, gestionar y mitigar de manera efectiva cualquier incidente de seguridad que pueda afectar la integridad, disponibilidad o confidencialidad de la información.

Unibac adopta un enfoque preventivo mediante:

- Ciberseguridad Avanzada con IA/ML: Implementación de soluciones para la detección temprana de anomalías y respuesta automatizada a incidentes.
- Equipo de Respuesta: Designación de roles claros para la contención de brechas y la investigación forense digital.
- Análisis de Vulnerabilidades: Escaneos periódicos de la red y aplicaciones para identificar debilidades antes de que sean explotadas.
- Indicadores de Éxito: Medición del tiempo de respuesta desde la detección hasta la contención del incidente.