INSTITUCIÓN UNIVERSITARIA
MAYOR DE CARTAGENA

AVANZA
HACIA LA EXCELENCIA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Elaborado por:

Equipo de Soporte y Desarrollo Tecnológico, 2024

Contenido

INTRODUCCION

Con el objetivo de fomentar una cultura de uso responsable y seguro de las tecnologías de la información y las comunicaciones dentro de nuestra institución, se han establecido políticas y directrices que deben regir nuestras acciones.

Este documento presenta un conjunto de Políticas y Lineamientos para el uso apropiado de los recursos y servicios de Tecnología de la Información y Comunicaciones (TIC) disponibles en la institución, dirigidos a estudiantes, docentes y todo el personal vinculado, sin importar la modalidad de su relación con la institución. Estas políticas se consideran herramientas clave para el desarrollo eficiente de nuestras actividades, al tiempo que protegen la seguridad y privacidad de la información.

En el contexto de la Política de Gobierno Digital formulada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), todas las entidades están obligadas a establecer mecanismos que permitan traducir los principios de las TIC en acciones concretas.

El propósito de estas políticas es salvaguardar la integridad de los recursos informáticos, incluyendo computadoras, redes, sistemas de información, software, programas y datos de propiedad institucional, incluso cuando no se encuentren físicamente en nuestras instalaciones, siempre y cuando cuenten con la autorización correspondiente. Esto se hace con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

Asimismo, se busca garantizar que el uso de dichos recursos esté en conformidad con las leyes, normativas y procedimientos tanto de la institución como de la República de Colombia.

Es fundamental subrayar que el uso de los recursos informáticos implica automáticamente la aceptación de estas políticas. Por lo tanto, es responsabilidad de cada individuo revisarlas y comprometerse a apoyar el correcto funcionamiento de los recursos informáticos bajo su custodia.

OBJETIVOS

- Establecer lineamientos o directrices para las políticas de seguridad de la información y la comunicación.

- Cumplir con los principios de privacidad y seguridad de la información.

- Promover la conciencia, capacitación y colaboración en buenas prácticas de seguridad de la información entre todos los usuarios de la Institución.

- Salvaguardar los activos informáticos tanto de hardware como de software frente amenazas internas o externas y accidentales, con el fin de asegurar el cumplimiento de las características de confiabilidad, confidencialidad, disponibilidad, integridad, legalidad y no repudio de la información.

- Definir un lenguaje común sobre la seguridad de la información y la ciberseguridad dentro y fuera de la institución.

- Mantener la política de seguridad de la información actualizada, operativa y vigente para asegurar su permanencia y nivel de eficacia.

- Cumplimiento en lo Fundamentados en el artículo 15 de la Constitución Política de Colombia, en la Ley 1581 de 2012 y en los decretos reglamentarios 1377 de 2013 y 886 de 2014 – hoy contenidos en los capítulos 25 y 26 del Decreto único 1074 de 2015, que desarrollaron el marco general de protección de datos en Colombia; La INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA, ha implementado las presentes Políticas de Tratamiento de Datos Personales por la cual se regirán todas las áreas de la Institución y los terceros a quienes se encargue el tratamiento de datos personales suministrados, con el fin de respetar todos los derechos y garantías en cuanto a privacidad de los titulares de la información suministrada.

ALCANCE

La política de seguridad de la información se aplica a todos los usuarios, recursos y actividades relacionadas con la tecnología de la información y las comunicaciones en la UMAYOR. Esto incluye, pero no se limita a, estudiantes, docentes, personal administrativo y cualquier otra persona que tenga acceso a los sistemas, redes y datos de la institución.

Las medidas de seguridad descritas en esta política abarcan todos los aspectos relevantes de la gestión de la seguridad de la información, incluyendo la protección de los activos de información, la gestión de accesos y contraseñas, la prevención de pérdida de datos, la detección y respuesta ante incidentes de seguridad, así como el cumplimiento de las regulaciones y normativas aplicables en materia de privacidad y protección de datos.

Esta política se implementará de manera integral en todas las áreas de la institución, independientemente de su ubicación física o modalidad de operación. Se proporcionarán recursos y capacitación adecuados para garantizar la comprensión y el cumplimiento de las disposiciones establecidas en esta política por parte de todos los usuarios.

La política de seguridad de la información se revisará periódicamente para garantizar su relevancia y eficacia continua en el entorno cambiante de amenazas y tecnologías. Los cambios y actualizaciones se comunicarán de manera oportuna a todos los interesados, y se brindará el apoyo necesario para su implementación adecuada.

La oficina de Sistemas y Desarrollo Tecnológico es la encargada de administrar y desarrollar las políticas de TICs, en la UMAYOR.

Cartagena de Indias - Centro histórico
Cr 3 # 35-95 Calle de la Factoría.
Umayorctg umayorctg UMAYOR

ST-PT-001 - POLITICA DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO A EQUIPOS DE CÓMPUTO

PROPOSITO: El propósito de esta política es brindar y coordinar los servicios necesarios de mantenimiento preventivo y correctivo para la infraestructura tecnológica e informática de la Institución Universitaria Mayor de Cartagena, con el objetivo de prolongar su vida útil, asegurar su óptimo funcionamiento y garantizar la seguridad de la información contenida en dichos equipos.

GENERALIDADES:

El Procedimiento se realiza a los equipos que se encuentran en las diferentes dependencias de la UMAYOR, con herramientas para garantizar el óptimo funcionamiento de estos, garantizando la disponibilidad de todos los computadores de la Institución.

DEFINICIONES:

APOYO A LA HISTORIA: Todas las solicitudes de apoyo y las respuestas son archivadas.

SOPORTE POR WEB Y CORREO ELECTRÓNICO: Cada vez que se gestiona una solicitud, el sistema crea un código (ticket) y es notificada por correo electrónico. Este código sirve para hacer seguimiento de la solicitud que llega a la mesa de ayuda tanto por el usuario como por el grupo de soporte.

MANTENIMIENTO PREVENTIVO: Se implementan mecanismos preventivos con el fin de mantener los equipos informáticos funcionando de manera óptima y segura. Esto incluye revisiones periódicas, actualizaciones de software antivirus y del sistema operativo, verificación de la sincronización de copias de seguridad, entre otras acciones destinadas a mitigar riesgos de seguridad de la información.

MANTENIMIENTO CORRECTIVO: Se llevan a cabo acciones para corregir fallas identificadas en los equipos de cómputo de manera eficiente y segura, priorizando la recuperación de la funcionalidad del sistema y la protección de la información.

ACTIVIDADES DE MANTENIMIENTO PREVENTIVO:

a. La oficina de Soporte y Desarrollo tecnológico realiza un mantenimiento preventivo semestralmente a todos los equipos de cómputo de la UMAYOR que se encuentran oficialmente inventariados por el departamento Infraestructura Física.
b. El equipo de Soporte y Desarrollo Tecnológico elabora un cronograma de mantenimiento preventivo de equipos de cómputo. Este cronograma de mantenimiento de equipos informáticos se registra en un formato FS-ST-003.
c. Los insumos necesarios para el mantenimiento preventivo son suministrados por la oficina de compras, asegurando la disponibilidad de recursos para llevar a cabo las actividades planificadas.
d. Se notifica a las dependencias de UMAYOR sobre las fechas programadas para los mantenimientos de equipos de cómputo, priorizando la coordinación y minimizando posibles interrupciones en las operaciones.
e. El director de Soporte y Desarrollo Tecnológico delega a los técnicos de sistemas la ejecución del cronograma de mantenimiento preventivo.
f. Los técnicos de sistemas llevan a cabo el mantenimiento preventivo de acuerdo con el cronograma establecido, realizando inspecciones detalladas, validación de registro del equipo de cómputo en la herramienta ESET Protect, actualizaciones de software antivirus, sistema operativo, verificación de la sincronización de copia de seguridad, limpieza física de los equipos y cualquier otra acción necesaria para garantizar el óptimo funcionamiento y la seguridad de los sistemas informáticos de la institución.
g. El técnico de Soporte y Desarrollo Tecnológico registra el mantenimiento preventivo en el formato FS-ST-003. Igualmente, se registra en el sistema de tickets ingresando al enlace http://was.umayor.edu.co para dar por concluido el servicio técnico.
h. Finalmente, se envía una encuesta de satisfacción diseñada en Formulario de Google a todas las dependencias que se beneficiaron con el servicio de mantenimiento preventivo.

ACTIVIDADES DE MANTENIMIENTO CORRECTIVO:

a. Tras ocurrir una falla de hardware o software en un equipo de cómputo, los funcionarios y/o contratistas de la UMAYOR deben solicitar el servicio de

mantenimiento correctivo a través de la mesa de ayuda Umayor ingresando al enlace http://was.umayor.edu.co. Para cada solicitud de soporte se le asigna un numero de ticket único. También los funcionarios y/o contratistas pueden reportar incidencias que requieran rápida solución mediante los espacios de chat en el correo institucional, luego de ser atendida, se documenta el proceso de solución de problemas en la mesa de ayuda.

b. Para crear un ticket es necesario que el funcionario o contratista de UMAYOR cuente con una cuenta de usuario en la plataforma WAS y un correo institucional para dar respuesta a la solicitud del mantenimiento. Al correo electrónico se le enviará el número de ticket y le mostrará un vínculo en el cual podrá consultar el estado de su solicitud.

c. Cada solicitud de soporte se le asigna a un número de Ticket único que se puede utilizar para rastrear el progreso y respuestas en línea, garantizando la trazabilidad y la seguridad de la información intercambiada.

d. Los técnicos de Soporte y Desarrollo Tecnológico deben dar solución a los tickets en el menor tiempo posible.

e. Los técnicos de Soporte y Desarrollo Tecnológico realizan un diagnóstico exhaustivo de las fallas reportadas en los tickets de mantenimiento correctivo, identificando las causas subyacentes y determinando las acciones necesarias para resolver eficientemente los problemas detectados.

f. Si al atender el ticket se encuentran fallas en el equipo de cómputo que requieran el reemplazo de una de sus piezas, la Oficina de Soporte y Desarrollo Tecnológico cuenta con repuestos provenientes de equipos dados de baja para efectuar la sustitución de las partes defectuosas. En caso de no contar con los repuestos necesarios, se procederá a solicitar la adquisición de los mismos a través de la oficina de Infraestructura física para que realicen la compra del mismo.

RESPONSABILIDADES DEL EQUIPO DE SOPORTE Y DESARROLLO TECNOLOGICO:

a. El equipo de Soporte y Desarrollo Tecnológico garantizará el mantenimiento y la gestión adecuada del Directorio Activo de la institución, incluyendo la creación, modificación y eliminación de cuentas de usuario, así como la administración de los permisos de acceso, asegurando la integridad y seguridad de la información almacenada en este sistema centralizado de autenticación y autorización.

b. Se establece la responsabilidad de proteger la información personal durante los procesos de mantenimiento, evitando la eliminación accidental o no autorizada de datos.

c. Se limita la instalación de programas a aquellos autorizados y necesarios para el desempeño laboral o académico, garantizando la integridad y seguridad de los sistemas informáticos.
d. Se reserva el derecho de instalar y desinstalar programas exclusivamente al equipo de Soporte y Desarrollo Tecnológico, con el fin de mantener la seguridad y el rendimiento de los sistemas.
e. Se establece un proceso formal para solicitar la instalación de programas específicos, asegurando que sean compatibles con las políticas de seguridad de la información y las necesidades institucionales.
f. Se prohíbe la instalación de programas sin licencias originales y sin autorización previa, con el fin de evitar riesgos de seguridad y cumplir con las regulaciones de propiedad intelectual.
g. La instalación de programas, ya sean de código abierto (open source) o específicos solicitados por funcionarios, contratistas o estudiantes, en los equipos de cómputo de la institución estará sujeta a una revisión y autorización previa por parte de la Oficina de Soporte y Desarrollo Tecnológico. Se garantizará que dichos programas cumplan con los estándares de seguridad y compatibilidad establecidos, así como con las políticas institucionales, con el fin de mantener la integridad y estabilidad de los sistemas informáticos.
h. Durante el mantenimiento preventivo o correctivo, el Equipo de Soporte y Desarrollo tiene la facultad de desinstalar todo programa que haya sido instalado por el funcionario, contratista o estudiante sin la autorización previa del jefe de área.

Cartagena de Indias - Centro histórico
Cr 3 # 35-95 Calle de la Factoría.
Umayorctg umayorctg UMAYOR

ST-PT-002 - POLITICA DE PROTECCIÓN DE RECURSOS INFORMATICOS

PROPOSITO: Salvaguardar la integridad y disponibilidad de los recursos informáticos, incluyendo equipos de cómputo, periféricos y dispositivos de almacenamiento, mediante la implementación de medidas de seguridad adecuadas. Esta política tiene como objetivo principal garantizar la confidencialidad, integridad y disponibilidad de la información, así como promover el uso seguro y responsable de los recursos informáticos por parte de todos los usuarios y administradores de la institución.

LINIAMIENTOS:

Responsabilidad y Custodia:

a. Todo funcionario, contratista o estudiante de UMAYOR es responsable de velar por el adecuado manejo, uso, control y custodia de los recursos informáticos asignados o utilizados en el desarrollo de sus actividades laborales o académicas.

b. Cada usuario deberá proteger sus credenciales de acceso y notificar de inmediato cualquier incidente de seguridad o pérdida de información a la Oficina de Soporte y Desarrollo Tecnológico.

Uso Autorizado:

a. Los recursos informáticos de UMAYOR solo pueden ser utilizados para actividades y funciones correspondientes al cargo o labor del usuario.

b. Antes de hacer uso de un equipo de cómputo perteneciente a otro usuario, es obligatorio obtener la autorización previa del usuario responsable del equipo o del jefe de área al cual pertenece el equipo y notificar esta acción a la Oficina de Soporte y Desarrollo Tecnológico.

c. Queda prohibido el uso de recursos informáticos para fines personales o actividades no relacionadas con las funciones laborales o académicas.

Ambiente de Trabajo Seguro:

a. Se prohíbe fumar, comer o beber en áreas donde se encuentren los recursos tecnológicos para evitar daños eléctricos y riesgos de contaminación.

b. Los equipos de cómputo deben ubicarse en lugares que brinden protección contra la humedad y el calor para garantizar su óptimo funcionamiento.

Gestión y Mantenimiento:

a. Ningún usuario puede trasladar, conectar o desconectar equipos de cómputo sin la debida autorización y supervisión de la Oficina de Soporte y Desarrollo Tecnológico.

b. La instalación o cambio de cualquier dispositivo de hardware debe ser comunicada previamente a la Oficina de Soporte y Desarrollo Tecnológico para su autorización y registro.

Buen Uso del Software:

a. El buen uso del software es fundamental para garantizar la seguridad y el rendimiento óptimo de las aplicaciones y programas.

b. Se prohíbe el ingreso a páginas web de redes sociales, violencia, videojuegos y cualquier contenido nocivo para los equipos y los usuarios.

c. Todo dispositivo externo conectado a los equipos de cómputo debe ser escaneado por el antivirus previamente a su uso para prevenir riesgos de seguridad.

Respuesta a Incidentes:

a. Se establecerá un procedimiento claro y eficiente para la gestión de incidentes de seguridad informática, que incluya la notificación, investigación, mitigación y seguimiento de los incidentes reportados.

b. Se designará un equipo de respuesta a incidentes de seguridad informática encargado de coordinar las acciones necesarias para hacer frente a las amenazas y vulnerabilidades.

Educación y Concientización:

a. Se implementarán programas de educación y concientización en seguridad informática para todos los usuarios y administradores, con el fin de promover buenas prácticas y crear una cultura de seguridad dentro de la institución.

Evaluación y Mejora Continua:

a. Se realizarán evaluaciones periódicas de la efectividad de las medidas de seguridad implementadas, con el fin de identificar áreas de mejora y actualizar la política según sea necesario para hacer frente a nuevas amenazas y vulnerabilidades.

ST-PT-004 - POLÍTICA PARA COPIAS DE SEGURIDAD Y RESTAURACIÓN

PROPOSITO:

Garantizar la integridad, disponibilidad y confidencialidad de los datos críticos de la Institución Universitaria Mayor de Cartagena. Esto se logra mediante la implementación de procedimientos sistemáticos y regulares para respaldar y almacenar de manera segura la información importante. La política establece directrices claras sobre la frecuencia de las copias de seguridad, los tipos de datos a respaldar, los métodos de almacenamiento adecuados y los protocolos de recuperación en caso de pérdida de datos. Además, busca minimizar el riesgo de interrupción del negocio y proteger contra amenazas como la pérdida de datos, la corrupción de archivos y los ataques cibernéticos.

Además, define roles y responsabilidades, y promueve pruebas regulares de recuperación para garantizar la efectividad de las medidas de seguridad.

GENERALIDADES:

La política de copias de seguridad de la institución tiene como objetivo principal garantizar la protección integral de la información crítica generada en cada estación de trabajo y en los sistemas críticos alojados en el data center. Esta política se establece para asegurar la integridad, disponibilidad y confidencialidad de los datos, así como para mantener la continuidad operativa frente a posibles incidentes. Se implementan procedimientos automáticos para respaldar los datos de cada usuario, tras acuerdos previos, y se realizan copias de seguridad en la nube de Google Drive y en dispositivos de almacenamiento aislados de la red. La política también promueve la colaboración con los usuarios para determinar qué datos son críticos y deben ser incluidos en el proceso de copias de seguridad, así como la implementación de medidas de seguridad adecuadas para proteger los datos contra amenazas internas y externas.

DEFINICIONES:

Copias de seguridad automáticas: Se refiere al proceso automatizado de respaldar los datos de manera programada y sistemática, sin intervención manual, con el fin de garantizar la protección de la información crítica.

Data center: es una instalación física donde se alojan y gestionan los servidores, sistemas de almacenamiento y otros equipos de tecnología de la información de una organización, incluyendo infraestructura para la administración y respaldo de datos.

Integridad de los datos: Hace referencia a la calidad de los datos, asegurando que la información no ha sido alterada de manera no autorizada o accidental, y que permanece completa y precisa a lo largo del tiempo.

Sincronización: Es el proceso de asegurarse de que los datos en dos o más ubicaciones estén actualizados y coincidan entre sí en tiempo real o con cierta periodicidad, garantizando la consistencia de la información.

Continuidad operativa: Se refiere a la capacidad de una organización para mantener sus operaciones y servicios incluso ante situaciones adversas o emergencias, como pérdida de datos, fallos de sistemas o desastres naturales, gracias a la implementación de planes de contingencia y medidas de recuperación de datos.

Servidor: Ordenador que proporciona servicios en una red.

RESPONSABLES:

La oficina de Soporte y Desarrollo Tecnológico de la Institución es el responsable de la implementación y supervisión del proceso de copias de seguridad, encargado de garantizar la adecuada configuración y funcionamiento de los sistemas de respaldo.

Usuario final: responsable en la colaboración activa en la identificación de los datos críticos y en el seguimiento de las políticas establecidas para asegurar la integridad y disponibilidad de la información.

LINEAMIENTOS

Procedimiento con el usuario final:

a. El equipo de Soporte y Desarrollo Tecnológico procede concertar visita técnica con los usuarios finales para explicarles el proceso de acuerdo y la importancia de proteger sus datos a través de copias de seguridad.

b. Se identifican los directorios, archivos que contienen información esencial para las operaciones del usuario final y se registran para su inclusión en el proceso de copias de seguridad.
c. El equipo de soporte y desarrollo tecnológico procede a configurar las copias de seguridad automatizadas según los requerimientos y directorios especificados por el usuario final.
d. Se formaliza el procedimiento en un acta: FT-ST-001 ACTA DE CONFIGURACIÓN DEL SISTEMA DE COPIA DE SEGURIDAD EN ÁREA DE TRABAJO.
e. El acta es revisada y firmada por el usuario final y el representante del equipo de Soporte y Desarrollo Tecnológico, para formalizar el compromiso de proteger los datos.
f. Se realizan pruebas periódicas para verificar que las copias de seguridad se estén realizando correctamente y que los datos críticos estén siendo respaldados de manera adecuada.
g. Se llevan a cabo pruebas de restauración de copias de seguridad de manera periódica para asegurar que los datos puedan ser recuperados de manera efectiva en caso de pérdida o daño.
h. El usuario final, tiene la obligación de reportar de inmediato por los medios institucionales (correo electrónico, chat institucional y/o mesa de ayuda) cualquier inconveniente en la sincronización de la copia de seguridad.
i. Las personas que tengan bajo su responsabilidad la administración de los elementos de cómputos e información tecnológica están obligadas a entregar a un tercero los lineamientos y los soportes por medio de actas de empalme en la entrega de la información asignado por la dirección.

Procedimiento en los sistemas críticos alojados en el data center:

a. El director de Soporte y Desarrollo Tecnológico, en conjunto con el Coordinador de Redes y Seguridad, identifican los sistemas críticos que requieren copias de seguridad, incluyendo configuración de routers críticos,

servidores virtuales, bases de datos, código fuente, y otros sistemas de información esenciales para la operación de la institución.

b. Se programan las tareas de copia de seguridad mediante la red, consolidándolas en un servidor de copia de seguridad y al mismo tiempo se programa las copias de seguridad en dispositivos de almacenamiento físico aislados de la red.

c. Se configura en el servidor de copias de seguridad, la herramienta de sincronización para realizar copias de seguridad automáticas de los sistemas críticos en la nube con una periodicidad diaria.

d. La custodia de los Backus de los sistemas críticos estarán bajo la administración de la oficina de Soporte y Desarrollo Tecnológico.

e. Se realizan pruebas regulares de recuperación o restauración de los sistemas de información a partir de una copia de seguridad y se documenta tal procedimiento. Todo ello, para asegurar que el procedimiento sea efectivo y los datos puedan ser restaurados rápidamente en caso de una emergencia.

Cartagena de Indias - Centro histórico
Cr 3 # 35-95 Calle de la Factoría.
Umayorctg umayorctg UMAYOR

ST-PT-005 POLITICA DE USO DE SOFTWARE

PROPOSITO: Esta política Normativa tienen como propósito establecer el uso de los equipos de cómputos institucionales para la administración de los programas (Licencias de Funcionamiento), adquiridas por parte de la UMAYOR.

GENERALIDADES:

A través de la adquisición de licencias de software, UMAYOR facilita al Usuario su utilización para la realización de las tareas inmersas en procesos institucionales de carácter misional y de apoyo. En cualquier momento que el usuario no esté de acuerdo total o parcialmente con esta política, deberá abstenerse de usar el software.

UMAYOR declara que toda licencia de software que se entrega o se instala en los equipos de cómputo que forman parte del parque computacional de la institución, se encuentra protegido por derechos de propiedad intelectual que incluyen: derechos de autor Institucional.

LINEAMIENTOS:

- El funcionario, contratista o estudiante de la institución deberá utilizar los programas o comandos del sistema operativo instalados en los equipos de cómputo cuando tenga un buen conocimiento de ellos, de lo contrario, es posible que dañe su información y/o la de los demás.
- El funcionario, contratista o estudiante al no estar seguro del funcionamiento u origen de un archivo evite eliminarlo.
- El usuario reconoce y acepta que el uso de una licencia de software adquirida por la institución no le implica ningún derecho de propiedad sobre el mismo, ni sobre los productos que de su uso se deriven.

- El usuario se debe abstenerse de copiar, modificar, reproducir, distribuir o utilizar el software de cualquier forma con o sin fines de lucro a menos que se cuente con la autorización expresa y por escrito de la UMAYOR.
- El Usuario se compromete a seguir las instrucciones o recomendaciones que imparta UMAYOR, o personal autorizado por ella, relacionados con los mecanismos o procedimientos establecidos para el uso del software y licencias adquiridas por la UMAYOR, que le sean instaladas. El Usuario

  únicamente deberá seguir instrucciones impartidas por la UMAYOR o por quien ésta autorice**.**
- El software licenciado para la UMAYOR, bajo ninguna circunstancia debe proporcionarse a personas u organizaciones externas o usarse con fines de lucro.
- Todo software licenciado por la UMAYOR, solo será instalado en equipos de cómputo que formen parte de la infraestructura tecnológica de la institución, cumpliendo con las condiciones técnicas, y las cantidades adquiridas, según el licenciamiento que se haya adquirido o pactado.
- La UMAYOR a través de la Oficina de Soporte y Desarrollo Tecnológico y la asesoría de la Oficina Jurídica de la Institución; y en concordancia con la normatividad interna, las leyes nacionales o internacionales aplicables, así como de la presente política; definirá el marco disciplinario relacionado con el no acatamiento de los principios y lineamientos definidos en la Política o un sus procesos, procedimientos o guías asociados. Dicho marco deberá ser institucionalizado y estar disponible públicamente.
- La UMAYOR se reserva el derecho a negar el uso o retirar una licencia de software instalada, sin necesidad de previo aviso, por iniciativa propia o a petición de cualquier persona, que justifique debidamente, a aquellos Usuarios que den un uso indebido al software, o que incumplan total o parcialmente ésta política.

Cartagena de Indias - Centro histórico
Cr 3 # 35-95 Calle de la Factoría.
Umayorctg umayorctg UMAYOR

ST-PT-006 - POLITICA DE ADMINISTRACION DE LICENCIAS DE SOFTWARE

PROPOSITO: Una vez adquirida las licencias se mantienen en custodia de la oficina de Soporte y Desarrollo Tecnológico de la Institución en medios magnéticos e impresos, y clasificadas de acuerdo a las diferentes actividades y a los procedimientos que se realicen en Administración de Licencias con el fin de garantizar el manejo adecuado de las mismas.

DEFINICIONES:

LICENCIA DE SOFTWARE: Es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario del programa informático (usuario consumidor /usuario profesional o empresa), para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

SOFTWARE LIBRE: Es un software disponible para cualquiera que desee utilizarlo, copiarlo y distribuirlo, ya sea en su forma original o con modificaciones. Es importante no confundir software libre con software gratis, ya que este no puede ser modificado.

NORMATIVIDAD:

a. El software instalado en cada equipo de cómputo de propiedad del UMAYOR debe estar respaldado por su respectiva licencia de software.
b. Las licencias de software adquiridas por la UMAYOR deben tener su registro contable dentro de los activos de la institución.

c. La oficina de Soporte y Desarrollo Tecnológico es la responsable de controlar y administrar las licencias de software.
d. La oficina de Soporte y Desarrollo Tecnológico aprueba la instalación de software libre cuando sea justificado para cumplir actividades y funciones propias de la Institución.
e. El software de usuario cliente: administrativo, contratistas, docentes y estudiantes debe ser instalado únicamente por la Oficina de Soporte y Desarrollo Tecnológico.
f. La instalación de las licencias de software de equipos periféricos tales como cámaras, celulares, parlantes, Tablet, Disco duro Externo, etc., de propiedad

   de los usuarios, es responsabilidad de los mismos. Por tal motivo, los propietarios deben demostrar su legalidad.
g. La oficina de Soporte y Desarrollo Tecnológico debe administrar y custodiar los medios de instalación del software adquirido por el UMAYOR.
h. Cada nueva actualización de software generada, ocasionara la baja de la anterior versión. Por tal motivo, la Dirección administrativa hará los ajustes contables correspondientes dentro de los activos del UMAYOR
i. Las licencias instaladas oficialmente serán las que correspondan al registro llevado por la Oficina de Desarrollo Tecnológico; si por tal motivo un usuario instala software sin el registro y permiso de la oficina encargada deberá responder por su legalidad.

Cartagena de Indias - Centro histórico
Cr 3 # 35-95 Calle de la Factoría.
Umayorctg umayorctg UMAYOR

ST-PT-007 - POLITICA DE GESTION DE CUENTAS DE CORREO ELECTRONICO

PROPOSITO: Una vez solicitada la apertura de un correo electrónico Institucional, se asegura que se mantenga la privacidad de los mensajes de correo electrónico y el buen uso del sistema al suministrar este servicio a su personal vinculado.

GENERALIDADES:

El Correo Electrónico Institucional es proporcionado por la oficina de Soporte y Desarrollo Tecnológico con el objeto de apoyar las funciones de comunicación entre los funcionarios, contratistas y estudiantes de la institución. Se asignarán cuentas de correo institucional a partir del dominio umayor.edu.co (usuario@umayor.edu.co).

La creación de cuentas de correos está condicionada a la autorización del Director de la Unidad y a las políticas de uso que se mostraran más adelante.

El funcionario, contratista y estudiante de la institución, al hacer uso del servicio de correo electrónico institucional es responsable y acepta las condiciones de uso.

DIRECTRICES PARA LA CREACIÓN DE CORREO ELECTRÓNICO INSTITUCIONAL PARA FUNCIONARIOS Y CONTRATISTAS:

Las cuentas de correo institucionales seguirán un tipo de patrón a partir del tipo de vinculación del empleado. La institución maneja tres tipos de vinculación: Provisionalidad, Docente Ocasional Medio Tiempo o Tiempo Completo y Contratación por Prestación de servicios

Para los empleados de tipo Provisionalidad y Prestación de Servicios se crearán cuentas de correos genéricos por cargos y para los de tipo Docente Ocasiona Medio Tiempo o Tiempo Completo correos personalizados.

Los correos genéricos por cargos nos protegen de cambios futuros en el caso de que un empleado ya no forme parte de la institución por motivos de despido, ascenso, cambio de planes profesionales, etc. En este punto los correos genéricos llevan cierta ventaja ya que al contener el nombre del cargo (o puesto) pueden ser usados por el nuevo empleado sin afectar las comunicaciones entre los funcionarios, contratistas y contactos profesionales.

Para el caso, de los docentes ocasionales se crearán cuentas de correos personalizadas en vez de cuentas genéricas porque en el caso que el docente no siga laborando en la institución por cualquier motivo su información del correo no se le puede asignar a otro en reemplazo, sino que se crea un correo personalizado del nuevo docente ya que cada docente maneja grupos de estudiantes y actividades diferentes.

DIRECTRICES PARA LA CREACIÓN DE CORREO ELECTRÓNICO INSTITUCIONAL PARA ESTUDIANTES:

Las cuentas de correo electrónico institucional para estudiantes se crearán a partir del número de cedula una vez sea matriculado.

ASIGNACION Y RESPONSABILIDADES SOBRE EL USO DEL CORREO INSTITUCIONAL PARA FUNCIONARIOS Y CONTRATISTAS:

a. La oficina de Soporte y Desarrollo Tecnológico cuenta con un administrador de cuentas de correo institucional. Encargado de crear, modificar y suspender cuentas con la autorización previa del usuario de la cuenta y el jefe de área.
b. Las cuentas de correo institucional se crean bajo el dominio usuario@umayor.edu.co.

c. El nombre de la cuenta de correo institucional sigue unos parámetros establecidos por el manual que se diseñó para la creación de cuentas de correo UMAYOR. Se tiene en cuenta lo siguiente:

- Para docentes se crean cuentas personalizas siguiendo un formato establecido
- Para cargos administrativos se crean cuentas genéricas siguiendo un formato establecido

d. El administrador de cuentas de correo al crear un correo institucional de la UMAYOR establece una clave automática temporalmente que es entregada al usuario para saber cambiada en el nuevo inicio de sesión.

e. El correo institucional es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión de información masiva tipo spam o cadenas.

f. Los Funcionarios u contratistas de la UMAYOR son completamente responsables de todas las actividades realizadas con sus cuentas de acceso al buzón asignado por solicitud de su institución.

g. El correo institucional es de uso exclusivo del cargo del funcionario u contratista y de la dependencia en donde se encuentre. Es una falta grave facilitar su

cuenta de correo electrónico a personas no autorizadas. De lo contrario, la oficina de Soporte y Desarrollo Tecnológico procederá a eliminar la cuenta.

h. Toda información que sea trasmitida desde la cuenta de correo de cada funcionario u contratista de la UMAYOR, son responsabilidad exclusiva del titular de la cuenta, por lo que dichos contenidos no reflejan las preferencias o ideas de la institución.

i. El funcionario u contratista al enviar un correo institucional a 5 o más contactos debe enviarlo con copia oculta. La razón es que cuando colocas varios destinatarios en el campo *Para*, esos destinatarios ven todas las direcciones de email de los demás, violando la Ley Orgánica de Protección de Datos (LOPD).

j. Están completamente prohibidas las siguientes actividades:

- Utilizar el correo institucional para cualquier propósito comercial o financiero
- No se debe participar en la propagación de mensajes en cadena de índole: político, religioso, piramidal, pornográfico o temas similares.
- Distribuir de forma masiva mensajes con información o contenido inapropiado de la UMAYOR.

I. El uso indebido de las cuentas de correo institucional suministrado por la Oficina de Soporte y Desarrollo Tecnológico, así como la violación a las políticas de uso descritas, tendrá como consecuencia la desactivación temporal o permanente de las mismas.

ASIGNACION Y RESPONSABILIDADES SOBRE EL USO DEL CORREO INSTITUCIONALPARA ESTUDIANTES:

a. Las cuentas de correo institucional se crean bajo el dominio usuario@umayor.edu.co.

b. A cada estudiante le será asignada una cuenta de correo institucional de la UMAYOR y se le suministrará un nombre de usuario y contraseña para acceder a este servicio.
c. Los estudiantes de la UMAYOR son completamente responsables de todas las actividades realizadas con sus cuentas de acceso al buzón asignado por solicitud de su institución.
d. La cuenta de correo institucional del estudiante es de carácter personal e intransferible. Por tal motivo no debe usar ni entregar la cuenta a otro estudiante.
e. Hacer uso de los servicios de correo institucional de UMAYOR de manera prudente y exclusivamente para las actividades académicas que lo requieran.
f. No se debe emplear cuentas de correo personal para el envío de información académica, únicamente se debe emplear la cuenta de correo institucional asignada.
g. Queda prohibido el envío de información masiva, como cadenas de mensajes de cualquier tipo, además, propaganda de clase comercial, político, religioso, material audiovisual, contenido discriminatorio, ideologías terroristas, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para la UMAYOR. No enviar ni recibir archivos ejecutables, música y videos, que no tengan relación con las labores académicas.
h. Resguardar la información catalogada como confidencial por la UMAYOR, evitando el envío de este tipo de información a personas no autorizadas.
i. El estudiante debe proporcionar cambio de contraseñas seguras que no contengan datos personales.

j. En lo posible, el correo electrónico debe ser el medio por el cual se deben manejar las comunicaciones entre la UMAYOR y los estudiantes, disminuyendo el uso de documentación impresa; se recomienda al estudiante incluir al final de sus correos el mensaje: “No imprima este correo a menos que sea absolutamente necesario. El medio ambiente es cosa de todos”

k. El correo electrónico no reemplaza las plataformas de formación académica, por lo cual los estudiantes inscritos en cursos virtuales, continuarán presentando las tareas y demás actividades a través de la Plataforma Virtual.

l. No se debe hacer uso de la cuenta de correo institucional de estudiantes, para el registro en medios electrónicos de uso personal como foros, portales, blogs, particulares, únicamente puede hacerlo si estos medios corresponden a actividades estrictamente académicas.

m. No están permitidos los mecanismos y sistemas que intenten ocultar la identidad del emisor de correo.

n. Los estudiantes son responsables de todas las actividades realizadas con las cuentas de correo electrónico institucional para estudiantes, la UMAYOR no será responsable de las opiniones o contenidos enviados a través de este medio.

o. Cada estudiante es responsable de su cuenta de correo. La contraseña asignada para el ingreso a su correo electrónico es Personal e Intransferible, en consecuencia, el estudiante es el único responsable del uso y confidencialidad de sus elementos de autenticación y debe comprometerse a mantener su información segura y para su uso exclusivo.

ST-PT-008 - POLITICA DE GESTIÓN DE REDES E INTERNET

PROPOSITO: Con esta política formulamos controles que permitan minimizar el riesgo generado por el acceso a Internet y a redes públicas, el intercambio de medios de almacenamiento portátiles, el intercambio de información con instituciones externas, etc., los cuales exponen los sistemas de UMAYOR a la propagación interna y externa de software con código malicioso o nocivo, que comprometen directamente la integridad, la disponibilidad y la confidencialidad de la información procesada por cada uno de los componentes de la red.

NORMATIVIDAD

a. Toda información clasificada como confidencial de UMAYOR, ya sea de administrativos, docentes, contratistas o de estudiantes, no puede ser divulgada por internet o intranet sin la previa aprobación de los directivos.
b. El equipo de Soporte y Desarrollo Tecnológico otorga acceso a los servicios y plataformas como internet alámbrico e inalámbrico, plataforma virtual académica, plataforma administrativa, mesa de ayuda a criterio de la necesidad en cada área y solicitada por los coordinadores.
c. Algunas de estas plataformas son vía web por lo tanto en cada máquina debe estar instalado un navegador Google Chrome, recomendado por el personal de Soporte y Desarrollo Tecnológico.
d. Cada usuario tendrá asignada una credencial de acceso conformada por un usuario y una clave que debe ser solicitada previamente por los Directores,

Jefes o Coordinadores, al equipo de Soporte y desarrollo Tecnológico, a través de los procedimientos establecidos.

e. Queda prohibida la descarga, instalación y configuración de navegadores distintos al estándar definido por el equipo de Soporte y desarrollo Tecnológico.

f. Todos los funcionarios, contratistas y estudiantes pertenecientes a UMAYOR con autorización al uso y acceso a estos servicios deben ser utilizadas exclusivamente para fines laborales o académicos.

g. Las opiniones, las declaraciones políticas, y los asuntos no propios del Instituto, dirigidos a funcionarios, contratistas y público en general del sector oficial o gubernamental u otras compañías y organizaciones, no deben ser enviados a través de estos servicios.

h. Está prohibido el acceso a sitios con información que pueda contener material difamatorio, ofensivo, obsceno, vulgar, racista, pornográfico o subversivo.

i. Queda restringido el acceso a sitios de contenido multimedia (videos, música, emisoras online, etc.) debido al alto consumo de canal de Internet/Intranet. Únicamente se permite su uso a aquellos funcionarios u contratistas que por sus actividades requieran monitorear estos sitios externos y tengan previa aprobación del Jefe Inmediato y la autorización de la Oficina de Soporte y Desarrollo Tecnológico.

j. Queda restringido el uso indebido a sitios web tales como:

- Acceder a sitios de apuestas en línea o videojuegos
- Acceder y/o descargar material pornográfico u ofensivo
- Compartir en sitios web información propia de funcionarios, contratistas y/o estudiantes de UMAYOR sin la debida autorización de los mismos
- Descargar documentos o archivos sin tomar las medidas de precaución para evitar el acceso a las redes y equipos informáticos.
- Utilizar el servicio de intranet/internet para fines comerciales o financieros ajenos a UMAYOR
- Modificar las opciones de configuración y/o parámetros de seguridad a los navegadores instalados por UMAYOR.

k. La oficina de Soporte y Desarrollo Tecnológico dispone de portal cautivo como parte de las medidas de seguridad de la red de la UMAYOR. Este portal cautivo es para autenticar y controlar el acceso de los usuarios a la red, garantizando que solo aquellos autorizados puedan navegar por internet y acceder a los recursos de la universidad. Además, permitirá llevar

un registro de actividad de los usuarios y aplicar políticas de acceso basadas en roles y privilegios.

l. La oficina de Soporte y Desarrollo Tecnológico cuenta con un firewall local para bloquear el acceso a funcionarios, contratistas y estudiantes que intenten ingresar a sitios web no autorizados y también proteger los equipos de cómputo de UMAYOR contra ataques, amenazas y malware.

m. Todos los equipos de cómputo de UMAYOR deben contar obligatoriamente con el software Eset Endpoint Security instalado, y cualquier ajuste de seguridad o configuración adicional se aplicará de manera centralizada, a nivel de red, por parte de la oficina de Soporte y Desarrollo Tecnológico, garantizando así una gestión uniforme y eficiente de la seguridad informática en toda la universidad.

n. Los miembros de la oficina de Soporte y Desarrollo Tecnológico estarán en la capacidad de capacitar a todos los funcionarios, contratistas y estudiantes en las buenas prácticas del uso de internet.

ST-PT-009 - POLITICA PARA EL TRATAMIENTO DE DATOS PERSONALES

PROPOSITO: Con esta política protegemos la recolección, almacenamiento, uso, circulación, verificación de los datos y supresión de datos personales registrados en cualquier base de datos en la UMAYOR, brindando herramientas que garanticen la autenticidad, confidencialidad e integridad de la información.

ALCANCE:

La Política de la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA cubre todos los aspectos administrativos, organizacionales y de control que deben ser cumplidos por los directivos, funcionarios, contratistas, estudiantes, docentes y terceros que laboren o tengan relación directa con la universidad.

La Política de protección de datos se integrará con los manuales de procedimientos y cualquier actividad o proceso que implique el tratamiento de datos por parte de la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA en el desarrollo de su objeto social deberá ajustarse a esta directriz administrativa.

DESARROLLO DE LA POLÍTICA DE PROTECCIÓN DE DATOS

La INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA tendrá presente en todas sus actuaciones el debido respeto por la protección de datos personales. En

consecuencia, solicitará desde el ingreso del dato, autorización para el uso de la información que reciba para las finalidades propias de su objeto misional.

La UMAYOR, acata los principios establecidos en la ley y atenderá en sus actuaciones y manejo de información de datos personales las finalidades que se deriven de la recolección de los mismos. De la misma forma, informará a todos sus usuarios los derechos que se derivan de la protección de datos personales.

DEFINICIONES:

Conformidad con la ley vigente sobre la materia, se establecen las siguientes palabras contenidas en las Políticas de Tratamiento de Datos Personales de la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA, las cuales serán aplicadas e implementadas acogiendo los criterios de interpretación que garanticen una aplicación sistemática e integral. De tal forma, que deberán entenderse en el siguiente sentido:

Aviso de Privacidad: Es el documento físico, electrónico o en cualquier otro formato, generado por la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA dirigido al Titular para informarle que le serán aplicables las presentes Políticas de Tratamiento de Datos Personales, como puede conocer su contenido, y que finalidad se dará a sus datos personales.

Base de Datos: Es el conjunto organizado de datos personales que sean objeto de Tratamiento, e incluye archivos físicos, electrónicos y automatizados.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables.

Dato Sensible: Aquel dato que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Encargado del Tratamiento de datos personales: Son las personas naturales o Jurídicas que por sí mismas o en asocio con otros, realicen el tratamiento de datos personales por cuenta de la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA-

Responsable del Tratamiento de datos personales: La INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA actúa como responsable frente a todos los datos personales sobre los cuales decida directamente que tratamiento les dará según las autorizaciones otorgadas por los Titulares.

Titular de datos personales: Persona natural cuyos datos personales son objeto de Tratamiento por parte de la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA.

Las personas que podrán ejercer los derechos establecidos en la Ley son:

1. El Titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición de la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA.

2. Sus causahabientes, quienes deberán acreditar dicha calidad.

3. Los representantes en caso que el Titular sea menor de edad o por medio de apoderado, previa acreditación de la representación o apoderamiento.

4. Por estipulación a favor de otro o para otro.

Tratamiento de datos personales: Es cualquier operación o conjunto de operaciones sobre los Datos Personales que realice la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA o los Encargados del Tratamiento por cuenta de la empresa tales como la recolección, almacenamiento, uso, circulación o supresión.

Transferencia de datos personales: Ocurrirá cuando la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA y/o los Encargados, envíen los datos personales a un receptor que, a su vez, es responsable del Tratamiento y que puede estar ubicado en Colombia o en el Exterior.

Transmisión de datos personales: Es la comunicación de los datos personales a un Encargado del Tratamiento, dentro o fuera de Colombia, con el propósito que este realice un Tratamiento por cuenta de la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA.

Oficial de Privacidad: Es la persona designada por la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA que tiene como funciones, entre otras, la protección de los datos personales de los titulares, la vigilancia y control

de la aplicación de la presente Política de tratamiento de Datos Personales y dar trámite a las solicitudes de los titulares que quieran ejercer los derechos a que se refiere la ley 1581 de 2012 y el presente documento. El Oficial de Privacidad podrá tener otros cargos dentro o fuera de la institución siempre y cuando cumpla de cabalmente con las funciones encomendadas mediante contrato, manual de funciones del oficial de privacidad o la ley 1581 de 2012.

PRINCIPIOS RECTORES:

Principio de Legalidad en materia de Tratamiento de datos: El tratamiento de datos es una actividad regulada que debe sujetarse a lo establecido en la ley.

Principio de Finalidad: Todas las actividades de acopio, procesamiento y divulgación de la información debe obedecer a una finalidad legítima de acuerdo con la Constitución Política de Colombia, y las normas que la regulen, la cual debe ser informada al Titular, definida en forma clara, suficiente y previa.

Principio de Libertad: Todas las actividades de registro y divulgación de los datos personales sólo pueden ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

Principio de Veracidad o Calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error, además deberá promoverse la actualización de los mismos.

Principio de Transparencia: En el tratamiento debe garantizarse el derecho del Titular a obtener del Responsable de dicho tratamiento o del Encargado, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Principio de Acceso y Circulación Restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales y de las disposiciones constitucionales y legales. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento

restringido sólo a los Titulares o terceros autorizados conforme a lo dispuesto citada ley.

Principio de Seguridad: La información sujeta a tratamiento por el Responsable del Tratamiento o Encargado del tratamiento a que se refiere la ley se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros, y evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento a la base de datos personales.

Principio de Confidencialidad: Todas las personas que intervengan en el tratamiento de datos personales que no tengan el carácter de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la Ley y en los términos de la misma.

FINALIDAD TRATAMIENTOS DE DATOS PERSONALES:

Se entiende por finalidad el propósito para el cual han sido recolectados los datos de las personas. El tratamiento y la finalidad que se dé a los datos personales por

parte **de la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA** y/o los encargados deberán ser los establecidos en la respectiva autorización otorgada por el Titular.

El tratamiento para los datos personales indispensables de estudiantes, docentes, trabajadores y/o contratistas, egresados estará enmarcado en el orden legal y en virtud de la condición de la Institución de educación superior, serán necesarios para el cumplimiento de la misión institucional de docencia, investigación y extensión.

De conformidad con lo establecido en el Art. 2.2.2.25.3.1, núm. 2 del Decreto 1074 de 2015, se informa que las finalidades para las que se obtienen los datos, se encuentran señaladas en el Aviso de Privacidad de la Institución, así como en los formatos de obtención de la autorización de los titulares.

DERECHOS DE LOS TITULARES DE DATOS PERSONALES

Los Titulares de los Datos Personales registrados en las Bases de Datos de la INSTITUCIONTECNOLOGICA COLEGIO MAYOR DE BOLIVAR, tienen los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales. Estos derechos los podrán ejercer, entre otros, frente a Datos Personales parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado por el;

b) Solicitar prueba de la autorización otorgada a la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA salvo cuando se exceptúe expresamente como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012;

c) Ser informado por la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA o el Encargado del Tratamiento, previa solicitud, respecto del uso que se ha dado a sus datos personales; d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen

e) Solicitar a la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA la revocatoria escrito de conformidad con al Art. 15 de la Ley 1581 de 2012 y con el título VI de la Política de Tratamiento de Datos Personales, en los siguientes casos.

1. Cuando considere que los mismos no están siendo tratados conforme a los principios, deberes y obligaciones previstas en la Ley 1581 de 2012.

2. Cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recolectados de la autorización y/o la supresión de sus Datos Personales, mediante presentación de reclamo

3. Cuando se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recolectados.

Excepciones al Derecho de revocatoria de la autorización y/o la supresión de Datos Personales

Es importante aclarar a los Titulares de datos Personales cuya información repose en las bases de datos de la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA**,** que el derecho de cancelación no es absoluto y la Institución puede negar el ejercicio del mismo cuando:

a) El titular tenga un deber legal o contractual de permanecer en la base de datos.

b) La eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.

c) Los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular; para realizar una acción en función del interés público, o para cumplir con una obligación legalmente adquirida por el titular.

Datos personales sensibles:

La INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA, podrá realizar el tratamiento de datos personales sensibles siempre y cuando:

a) El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

b) El Tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

c) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

d) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

La INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA restringirá el tratamiento de datos personales sensibles a lo estrictamente indispensable y solicitará consentimiento previo y expreso sobre la finalidad de su tratamiento,

además de hacerlo bajo las más estrictas medidas de seguridad y confidencialidad.

Derechos de los niños, niñas y adolescentes:

En términos generales, la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA no realiza tratamiento de datos personales de niños, niñas y adolescentes, sin embargo, en casos excepcionales, podrá realizar el tratamiento de los mismos siempre y cuando:

1. Se trate de datos de naturaleza pública,

2. El tratamiento realizado por la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA responda y respete el interés superior de los niños, niñas y adolescentes.

3. El tratamiento realizado por la INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA asegure el respeto de sus derechos fundamentales.

Una vez cumplidos los anteriores requisitos, el representante legal de los niños, niñas o adolescentes otorgará la autorización, previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. La INSTITUCION UNIVERSITARIA MAYOR DE CARTAGENA se compromete entonces, en el tratamiento de datos personales, a respetar los derechos prevalentes de los menores. Queda proscrito el tratamiento de datos personales de menores, salvo aquellos datos que sean de naturaleza pública.

ST-PT-011- POLITICA DE ESCRITORIO DE TRABAJO Y PANTALLAS LIMPIAS

PROPOSITO: Prevenir la perdida, daño o robo de la información durante y fuera de la jornada laboral en las estaciones de trabajo, y salas informáticas, Bibliotecas, salones de diseños de arquitectura y electromecánica de la UMAYOR.

GENERALIDADES: Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política

de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, durante el horario normal de trabajo como fuera del mismo.

Las estaciones de trabajo se ubican de tal forma que no queden expuestas al acceso de personas externas, excepto la ventanilla única de la UMAYOR, para este caso en lo posible los monitores deben ubicarse de forma que no puedan ser visualizados por personas externas a la institución.

Los equipos de reproducción de información (impresoras, fotocopiadoras, escáneres, etc.), deben estar ubicados en lugares de acceso controlado y cualquier documentación con información pública clasificada o pública reservada se debe retirar inmediatamente del equipo y ser puesta en un lugar seguro.

DEFINICIONES:

Escritorio limpio: Protección de los papeles y dispositivos removibles de almacenamiento de información, almacenados y manipulados en estaciones de trabajo, de accesos no autorizados, perdida o daño de la información.

Estación de trabajo: Área designada por la organización para que cada colaborador pueda llevar a cabo sus actividades laborales. Esto incluye oficinas, escritorios y cualquier otro espacio equipado con los recursos necesarios para desempeñar sus funciones.

Lugar seguro: Es aquel que protege el activo de información de acceso de personas no autorizadas, que su contenido no sea alterado y que el activo pueda ser recuperado por las personas autorizadas de manera oportuna (algunos ejemplos son: cajón seguro con llave, oficina con llave, etc.)

Pantalla limpia: Protección de los equipos de cómputo, tabletas, portátiles u otros dispositivos mediante un bloqueo de pantalla o desconexión cuando no está en uso.

ACTIVIDADES PARA MANTENER ESCRITORIO LIMPIO

a. Todos los funcionarios y contratistas de la UMAYOR al ausentarse de su estación de trabajo u escritorio, deberá guardar en un lugar seguro y bajo llave documentos en medio físico, magnético u óptico que contenga información pública de uso interno, publica clasificada o publica reservada. Además, bloquear su equipo de cómputo mas no apagar la pantalla (Por

ejemplo, bloquear los equipos con sistema operativo Windows con las teclas **Windows + L**)

b. El funcionario y contratista, de la UMAYOR al imprimir documentos con información pública reservada y pública clasificada, deberá retirarlas inmediatamente de las impresoras.

c. Para el personal que está ubicado en zonas de atención al público, al ausentarse de su estación de trabajo o escritorio deberá también guardar en un lugar seguro y bajo llave los dos documentos y medios que contengan información pública de uso interno, publica clasificada o publica reservada.

d. Al finalizar la jornada de trabajo, los funcionarios y contratistas, deberán guardar en un lugar seguro y bajo llave los documentos y medios que contenga información pública de uso interno, publica clasificada o publica reservada. Además, apagar su equipo de cómputo.

ACTIVIDADES PARA MANTENER PANTALLAS LIMPIAS

a. La pantalla del equipo de cómputo (escritorio) debe estar libre de archivos o enlaces de acceso a archivos, estos deben ubicarse en las debidas carpetas

b. Todos los equipos de cómputo y portátiles de la UMAYOR deberán tener aplicado el cierre de sesión por inactividad. De esta manera, evitamos miradas indiscretas de personas cerca de nuestro entorno de trabajo.

c. Siempre que el personal se ausente de su estación de trabajo deberá bloquear todos los equipos y dispositivos que de él dependen y/o utiliza.

ST-PT-013 - POLITICA PERDIDA O HURTO DE RECURSOS TECNOLOGICOS

PROPOPOSITO: Establecer los lineamientos y actividades a realizar por perdida, robo o daño de los recursos tecnológicos de la Institución Universitaria Mayor de Cartagena, Con el fin de establecer las medidas legales de acuerdo a la situación presentada.

LINEAMIENTOS:

a. Los funcionarios, contratistas y estudiantes de la UMAYOR, son responsable del recurso tecnológico que se le asigne para la realización de las funciones propias que estén bajo su responsabilidad mientras esté vinculado con la Institución.

b. En caso de pérdida o hurto del recurso tecnológico, la reposición del equipo tecnológico será responsabilidad del usuario, siempre y cuando se demuestre su responsabilidad.

c. Todo evento, ajeno al buen funcionamiento del recurso tecnológico, debe ser informado una vez suceda mediante correo electrónico al Coordinador de Soporte y Desarrollo Tecnológico y al Jefe de Área, anexando las evidencias relacionadas al evento. Los eventos a reportar son:

- Robo
- Perdida
- Daño de equipo

d. Enviar a la oficina de Soporte y Desarrollo Tecnológico un correo electrónico informando el evento sucedido ya sea robo, perdida o daño de los recursos tecnológicos con la siguiente información:

- Marca de equipo a reportar
- Recurso Tecnológico: Portatil, PC, VideoBeam, impresora, escáner, multifuncional, Audífonos, Parlantes, Disco Externo, Memora usb, entre otras.
- Tipo de identificación del responsable del equipo a reportar
- Fecha del evento
- Descripción del evento junto con el denuncio respectivo del evento reportado.
- Anexos necesarios para reportar el evento
- La Oficina de Soporte y Desarrollo Tecnológico debe enviar un correo a la Directiva con la información anterior, la cual debe:
- Dar de baja el equipo o anexar la novedad al equipo reportado.

- Reportar a la empresa aseguradora el evento para gestión de este.
- Para la reposición del equipo la Dirección responsable debe realizar la solicitud de reposición a la Oficina de Soporte y Desarrollo Tecnológico mediante el formato “Solicitud de suministros y servicios”.

ST-PT-014 - POLITICAS DE USO DE LA PLATAFORMA VIRTUAL UMAYOR

PROPOSITO: La plataforma virtual es un servicio que la Institución Universitaria Mayor de Cartagena pone a disposición de sus estudiantes, docentes, administrativos y egresados como herramienta Tecnológica que servirá como apoyo a las clases presenciales.

GENERALIDADES: El presente documento es un reglamento del uso general de la plataforma virtual que deben seguir los usuarios de la misma y pretende ser un recurso para optimizar y asegurar el correcto funcionamiento de los recursos digitales involucrados durante todo el proceso de enseñanza y aprendizaje por medios virtuales.

AMBITO DE APLICACIÓN:

Las siguientes normas son de aplicación a todos los usuarios que accedan a la Plataforma Virtual UMAYOR:

- El acceso a la plataforma implica el conocimiento y la aceptación por parte del usuario de las normas de uso recogidas en este documento.
- Cada usuario es el único responsable del uso que haga de la Plataforma, de acuerdo con los términos aquí descritos.
- Los administradores funcionales de la Plataforma Virtual serán los encargados de la gestión de dicho Campus, velarán en todo momento por el correcto cumplimiento de los términos y condiciones de uso por parte de sus usuarios.
- Estas políticas podrán ser modificadas o bien para ajustarla a la evolución tecnológica o a cambios legislativos, o bien cuando la Institución Universitaria Mayor de Cartagena lo estime conveniente.

MEDIDAS DE SEGURIDAD:

Se considera usuario de la Plataforma Virtual a toda persona vinculada a la institución que se inscriba o matricule en uno o más cursos de la oferta educativa.

Acceso a la plataforma virtual

Para acceder a la plataforma virtual se debe ingresar desde el sitio web http://genesis2.umayor.edu.co/. El uso de los recursos tecnológicos desde los que se puede acceder a la plataforma virtual son responsabilidad del usuario y éste debe garantizar que la información digital que pudiera manipular en ese momento no sea visible por terceros no autorizados. Se sugiere que antes de dejar de utilizar o abandonar el recurso tecnológico por el cual accede a la plataforma, cierre la aplicación de la misma haciendo clic en el vínculo “salir”.

Usuario y contraseña

El usuario puede acceder al servicio por medio de una contraseña que es suministrada vía e-mail tras ser validados sus datos personales en el sistema. Se recomienda que bajo ninguna circunstancia sea revelada a terceros dicha información ya que todo daño o perjuicio que pudiera derivarse de este hecho serán atribuidos al usuario titular.

Imagen personal

Relacionar una fotografía con el usuario de la plataforma es responsabilidad exclusiva del usuario y es obligatoria. El usuario podrá subir una imagen personal siempre y cuando sea de su rostro y no atente contra las normas vigentes de la institución, de lo contrario la Institución Universitaria Mayor de Cartagena podrá retirarla sin previo aviso.

Revelación de datos e información

El usuario debe entender que, para efectos de verificación y validación de sus datos, el sistema también almacena todos los datos relacionados desde su vinculación con la institución, pero sólo son visibles en el entorno gráfico de la plataforma virtual el nombre y apellidos completos y el número de documento de identificación. Cualquier información personal revelada en espacios colectivos como foros, chats o blogs se publica bajo la exclusiva responsabilidad del usuario titular. Se recomienda que bajo ninguna circunstancia se revelen datos de ideologías, creencias, religión, origen racial, salud o vida sexual. La revelación de estos datos son responsabilidad exclusiva del usuario titular y por tanto la Institución Universitaria Mayor de Cartagena no asume ninguna responsabilidad u obligación por este hecho.

Material digital

El usuario es el único responsable por el material que sube a la plataforma. Queda terminantemente prohibido y bajo ninguna circunstancia subir material que incumpla con la legislación vigente en el tema de infancia y adolescencia, derechos de autor, propiedad intelectual y patentes. Todo material que pueda subir cumplidos los términos anteriores debe estar libre de virus y en formatos que impidan su modificación posterior al envío.

a. Existirá únicamente un administrador de la plataforma virtual.

b. El administrador de la plataforma virtual verificará que el docente que desea incorporar la utilización de la plataforma virtual UMAYOR como apoyo a la docencia presencial y/o curso de capacitación virtual cumpla con los siguientes requisitos:

- Formación previa del docente en temas relacionados con el modelo de educación B-Learning (se refiere a la combinación del trabajo presencial y del trabajo en línea).
- Conveniencia de la asignatura para ser apoyada por la virtualidad.
- Estructurar el curso, nombre de la asignatura, unidades y actividades.

USO ACADÉMICO DE LA PLATAFORMA

La plataforma virtual es un recurso para el aula de clases donde el docente y el estudiante puede seguir interactuando y complementado los procesos de enseñanza y aprendizaje. En ningún momento pretende reemplazar el espacio físico en el que docente y estudiante interactúan académicamente.

Obligaciones por parte del estudiante

En virtud del uso exclusivamente académico de la plataforma virtual, el estudiante se compromete a:

a. Acceder únicamente a los recursos digitales autorizados.

b. Comunicar a su docente o al coordinador de la plataforma virtual cualquier incumplimiento a las normas establecidas en el presente documento, durante el uso de esta.

c. Dirigirse con respeto hacia todo usuario de la plataforma virtual.

d. Hacerse responsable porque todo el material digital publicado desde su usuario no incumpla la legislación vigente.

e. Utilizar la plataforma virtual exclusivamente para actividades académicas.

f. Abstenerse de publicar y/o enviar spam o publicidad u otros fines no académicos, así como imágenes, videos o cualquier otro material multimedia con contenido pornográfico o que no tenga fines académicos.

g. Participar activamente en los foros que los docentes pongan a su disposición.

h. Desarrollar activamente las guías, talleres, evaluaciones y demás actividades que el docente ponga a su disposición.

i. Revisar las calificaciones de sus actividades en un plazo no superior a 5 días después de ser notificadas por su respectivo docente. Cumplido este plazo no se aceptarán reclamaciones de ninguna índole.

Obligaciones por parte del docente

La utilización del entorno virtual no exime al docente de cumplir con las horas presenciales correspondientes a la programación de la asignatura, en el caso de que se use como apoyo a la docencia. El docente podrá hacer uso de todos los recursos y actividades que la plataforma virtual ofrece para realizar el acompañamiento virtual de la asignatura que imparte. El material generado por cada docente en su aula virtual iría a un repositorio digital institucional bajo previa autorización del docente.

Para hacer uso de la plataforma Virtual todo docente deberá cumplir con los siguientes lineamientos:

a. El registró en la plataforma educativa se hará por parte del administrador de la plataforma, el docente completara su registro recordando que la información es personal e intransferible (Claves, datos personales).

b. El docente que desee incorporar el uso de la plataforma virtual a sus procesos de enseñanza-aprendizaje deberá basarse en la premisa de que cualquier apoyo en la tecnología para un curso presencial ya existente deberá ser considerado una mejora, que proporcionará un valor agregado tanto al docente como a la asignatura y al proceso de enseñanza aprendizaje. No sustituirá a lo que se tiene actualmente en la presencial, sino que lo complementará y enriquecerá.

c. El docente que haga uso de la plataforma virtual, tiene la obligación de:

- Dar apoyo a sus estudiantes en la realización de las actividades.
- Hacer el seguimiento a sus estudiantes dentro de la plataforma.
- Dar de baja a sus estudiantes una vez terminado el semestre o curso virtual.
- Sacar copia de seguridad de su aula.
- Informar en el plazo de un mes una vez finalizado el semestre o el curso al administrador de la plataforma virtual si se requiere mantener esta aula para el siguiente semestre o curso, caso contrario el aula será eliminada a los 6 meses.

d. El tamaño máximo de los archivos utilizados en la plataforma será de 4Mb, recordando que las imágenes deberán tener extensión jpg o png, los videos utilizados dentro de la plataforma serán subidos a la plataforma Youtube y de ahí solo se utilizara el link para su reproducción en la plataforma virtual.

e. Desarrollar y/o relacionar todo el material digital que suba y/o envíe a la plataforma virtual según la legislación vigente en los temas de derechos de autor, propiedad intelectual y patentes.

f. Comunicar a su director de Unidad o al coordinador de la plataforma virtual cualquier incumplimiento a las normas establecidas en el presente documento, durante el uso de la plataforma virtual.

g. Dirigirse con respeto hacia todo usuario de la plataforma virtual.

h. Utilizar la plataforma virtual exclusivamente para actividades académicas.

i. Abstenerse de publicar y/o enviar spam o publicidad u otros fines no académicos, así como imágenes, videos o cualquier otro material multimedia con contenido pornográfico o que no tenga fines académicos.

j. Proponer y desarrollar foros de consulta y debate dentro de la plataforma virtual, sin que estos incumplan las normas contempladas en el presente documento.

k. Proponer guías, talleres, evaluaciones y demás actividades en formatos digitales. Se sugiere que todo material digital que sea subido/enviado a la plataforma esté en un formato que no permita su modificación.

l. Elaborar copias de seguridad de las guías, talleres, evaluaciones y demás material que suba y/o envíe a la plataforma virtual.

m. Abstenerse de permitir reenvíos de una actividad por parte del estudiante.

n. Revisar y calificar toda actividad que el estudiante envíe en un plazo no superior a 10 días después de vencida la fecha de envío en la plataforma virtual y notificarle al estudiante esta acción.

LINEAMIENTOS Y RECOMENDACIONES PARA COORDINADORES

- La función del coordinador es muy importante en la gestión y seguimiento de este proyecto por lo que es necesario que asista a las reuniones de capacitación, planeación y evaluación que para este efecto se promueven.

- El coordinador verificara que los docentes estén haciendo uso de la plataforma virtual, comprobando periódicamente el montaje de materiales y unidades académicas.

- El coordinador debe favorecer los espacios a los docentes de reflexión y mejora de los programas y contenidos de la licenciatura con el grupo de asesores en su unidad y participar activamente en estos espacios.
- Asistir a las capacitaciones para el uso y administración de la plataforma virtual UMAYOR y promover y solicitar los espacios de capacitación requeridos para sus asesores en función de un mejor aprovechamiento de los recursos de la misma.

- Orientar y dar seguimiento académico y organizativo a los asesores de su coordinación y de forma específica, a los que utilicen la plataforma virtual UMAYOR durante cada cuatrimestre.

- Enviar en tiempo listado de docentes y estudiantes para de esta manera llenar los requerimientos de inscripción de docentes y matriculación de estudiantes.

RESPONSABILIDAD

La Institución Universitaria Mayor de Cartagena se compromete a no revelar los datos personales de sus usuarios y a no usarlos para fines comerciales y/o publicitarios. El uso de estos datos es exclusivo de la institución y serán usados con fines estadísticos y académicos. Cada usuario es responsable por el uso personal que realice de la información contenida u obtenida de las aulas virtuales y la UMAYOR no asume ninguna responsabilidad que se pueda derivar de problemas técnicos o fallos en los equipos informáticos que se produzcan durante la conexión a la red de Internet, así como de daños que pudieran ser causados por terceras personas mediante intromisiones ilegítimas fuera del control de la Institución Universitaria Mayor de Cartagena. También quedamos exonerados de toda responsabilidad ante posibles daños o perjuicios que pueda sufrir el usuario a consecuencia de errores, defectos u omisiones en la información que facilitemos cuando proceda de fuentes ajenas a nosotros.

PROPIEDAD INTELECTUAL

El proceso de enseñanza y aprendizaje por medios virtuales requiere de recursos tanto físicos como virtuales. Desde el punto de vista virtual, todo recurso usado/desarrollado para la plataforma de la Institución Universitaria Mayor de Cartagena se regirá de acuerdo a las disposiciones complementarias establecidas por la Institución.

ACTUALIZACIÓN Y MODIFICACIÓN DE LA PLATAFORMA VIRTUAL.

La Institución Universitaria Mayor de Cartagena se reserva el derecho a modificar o eliminar, sin previo aviso, tanto la información contenida en la plataforma virtual como su configuración y presentación, sin asumir responsabilidad alguna por este hecho.

Cartagena de Indias - Centro histórico
Cr 3 # 35-95 Calle de la Factoría.
Umayorctg umayorctg UMAYOR

ST-PT-015 - POLÍTICA DE GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

Propósito:

Establecer un marco integral y eficiente para la detección, notificación, evaluación, respuesta y recuperación ante incidentes de seguridad cibernética. Esta política tiene como objetivo principal garantizar la protección de los activos de información de la institución, la continuidad de las operaciones y la mitigación de los riesgos asociados con las amenazas cibernéticas.

Lineamientos:

1. **Definición de Incidentes:**

a. Se define como incidente de ciberseguridad cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de los sistemas de información de UMAYOR, incluyendo, pero no limitado a intrusiones no autorizadas, malware, ataques de denegación de servicio, y pérdida o robo de datos.

2. **Roles y Responsabilidades:**

a. Se designará un Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT), liderado por el Director de Soporte y Desarrollo Tecnológico, e integrado por los Programadores, Técnicos de Soporte y el Coordinador de Red y Seguridad.

b. El CSIRT será responsable de coordinar las actividades de gestión de incidentes, desde la detección hasta la resolución, y asegurarse de que se sigan los procedimientos establecidos.

3. **Procedimientos de Notificación:**

a. Todos los incidentes de ciberseguridad deben ser notificados de inmediato al CSIRT a través de los canales de comunicación institucional: d.sistemas@umayor.edu.co y redesyseguridad@umayor.edu.co

b. Todo incidente de ciberseguridad notificado a los canales institucionales debe proporcionar información detallada sobre la naturaleza del incidente, incluyendo la fecha y hora de detección, captura de pantalla y cualquier otra observación relevante para la investigación y mitigación del mismo.

c. Si el evento notificado corresponde a phishing (suplantación de identidad) recibido vía correo electrónico, el usuario está en la obligación de seguir los siguientes pasos:

- No interactuar con el remitente: Evita responder o hacer clic en enlaces adjuntos, especialmente si tienes dudas sobre la autenticidad del remitente o el contenido del mensaje.
- Reenviar el correo a: redesyseguridad@umayor.edu.co y d.sistemas@umayor.edu.co para su análisis por parte del equipo de seguridad informática.
- Denunciar el correo recibido como suplantación de identidad: Utiliza las opciones de reporte disponibles en tu cliente de correo electrónico para denunciar el correo como suplantación de identidad. Esto nos ayudará a identificar y bloquear futuros intentos de phishing.
- Eliminar el correo: Una vez que hayas reenviado el correo y lo hayas denunciado, elimínalo de tu bandeja de entrada para evitar posibles interacciones involuntarias.

4. Evaluación y Clasificación de Incidentes:

a. Se realizará una evaluación inicial de la gravedad y el impacto de cada incidente para determinar la respuesta adecuada.

b. Los incidentes serán clasificados según su nivel de gravedad y prioridad, de acuerdo con criterios predefinidos.

5. Respuesta y Recuperación:

a. Se implementarán medidas de respuesta inmediata para contener y mitigar el impacto del incidente, incluyendo la preservación de la evidencia digital relevante.

b. Se desarrollarán planes de recuperación para restaurar la funcionalidad normal de los sistemas afectados y minimizar el tiempo de inactividad.

6. **Análisis Post-Incidente:**

a. Se llevará a cabo un análisis exhaustivo de cada incidente de ciberseguridad para identificar las causas subyacentes, las lecciones aprendidas y las áreas de mejora.

b. Los resultados del análisis post-incidente se utilizarán para actualizar los procedimientos y fortalecer las medidas de seguridad cibernética de la institución.

7. **Educación y Concientización:**

a. Se promoverán programas de educación y concientización en seguridad cibernética para todos los empleados, contratistas y estudiantes de la UMAYOR, con el fin de fomentar una cultura de seguridad y buenas prácticas en el uso de los recursos informáticos.

b. Se realizarán campañas periódicas de concientización sobre el phishing, con el objetivo de educar a los usuarios sobre las técnicas utilizadas por los ciberdelincuentes y cómo identificar y evitar correos electrónicos y enlaces maliciosos.

8. **Revisión y Mejora Continua:**

a. La política de gestión de incidentes de ciberseguridad será revisada periódicamente para garantizar su efectividad y relevancia en un entorno cambiante de amenazas cibernéticas.

b. Se realizarán evaluaciones regulares de la capacidad de respuesta a incidentes y se implementarán acciones correctivas según sea necesario para mejorar la preparación y respuesta de la institución ante incidentes de seguridad cibernética.

9. Evaluación de Vulnerabilidades y Pruebas de Seguridad:

a. Se llevarán a cabo pruebas regulares de phishing, en las que se simularán ataques de phishing para evaluar la preparación y conciencia de los usuarios ante esta amenaza.

b. Los resultados de las pruebas de phishing se utilizarán para identificar las áreas de mayor riesgo y desarrollar planes de acción específicos para fortalecer la resistencia a este tipo de ataques.

c. Se proporcionará capacitación adicional a las dependencias identificadas como más propensas a caer en ataques de phishing, con el objetivo de mejorar la conciencia y respuesta de los usuarios ante estas amenazas.