UNIVERSIDAD DEL ROSARIO	**Circular Normativa**	**No. 186 SIND-2024**

CIUDAD Y FECHA: **Bogotá D.C, 28 de noviembre 2024**

PARA: **Comunidad Rosarista**

DE: **Sindicatura**

ASUNTO: **Políticas de Seguridad Informática aplicables para el Uso Aceptable y la Protección de los Recursos Informáticos de la Universidad del Rosario**

I. OBJETIVO

Establecer las políticas institucionales que regulen el uso y generen la protección a los recursos informáticos de la Universidad del Rosario, logrando mitigar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información.

II. ALCANCE

Aplica a todo el personal administrativo, estudiantes, egresados, profesores, invitados y demás usuarios que utilizan los recursos informáticos que provee la Universidad del Rosario para el ejercicio de sus actividades institucionales.

III. POLÍTICA GENERAL DE SEGURIDAD INFORMÁTICA

La información institucional es considerada por la Universidad del Rosario como un activo estratégico, convirtiéndose en un componente esencial e imprescindible que debe ser protegido para el cumplimiento de los objetivos institucionales, razón por la cual, la Universidad establece las siguientes políticas de seguridad informática aplicables para el uso aceptable y la protección de los recursos informáticos y su información como parte de una estrategia orientada a la administración de riesgos, a la continuidad de TI, la consolidación de una cultura de seguridad informática y el cumplimiento de los requerimientos internos, contractuales, legales y regulatorios vigentes

IV. POLÍTICAS ESPECÍFICAS DE USO ACEPTABLE Y PROTECCIÓN DE LOS RECURSOS INFORMÁTICOS

CAPÍTULO 1. Recursos Informáticos de la Universidad

Los usuarios administrativos, profesores, estudiantes, egresados, invitados y demás usuarios que utilizan los recursos informáticos de la Universidad deben:

1. Emplear los recursos informáticos proporcionados por la Universidad para los fines institucionales pertinentes, siendo responsabilidad del usuario hacer uso adecuado, seguro y eficiente de dichos recursos.

2. Proteger la información almacenada en los recursos informáticos contra acceso, modificación y divulgación no autorizada. Esta información es propiedad de la Universidad cuando se trate de usuarios administrativos, profesores y contratistas, salvo excepciones contractuales e información personal que sea identificada como tal.

3. Realizar tratamiento confidencial a las claves de acceso otorgadas para el uso de los recursos informáticos. Las claves de acceso son de uso personal e intransferible, siendo responsabilidad del usuario las acciones ejecutadas en los recursos informáticos con sus claves de acceso. De igual manera, deben:

   3.1 Configurar claves de acceso de manera robusta y difícil de acertar, con al menos (8) caracteres de longitud, combinando mayúsculas, minúsculas, números y caracteres especiales.

   3.2 Para personal administrativo y profesores se debe cambiar como máximo cada 3 meses las claves de acceso, sin repetir claves utilizadas anteriormente.

   3.3 Para estudiantes cambiar como máximo cada 7 meses las claves de acceso, sin repetir claves utilizadas anteriormente.

   3.4 Para egresados cambiar como máximo cada 12 meses las claves de acceso, sin repetir claves utilizadas anteriormente.

   3.5 Evitar digitar las claves de acceso para ingresar a los recursos informáticos de la Universidad desde conexiones de redes WIFI no seguras.

   3.6 Cambiar de manera inmediata las claves de acceso, cuando exista indicio de que esta ha sido expuesta y/o utilizada por otra persona.

   3.7 Cerrar inmediatamente las sesiones de las aplicaciones, sistemas de información, cuentas de correo y los demás recursos tecnológicos, una vez finalizado su uso.

   3.8 Reportar oportunamente a Servicios 2030 y/o a los canales que la Universidad haya definido para el efecto, cualquier sospecha de incidente de seguridad

relacionado con sus claves de acceso (robo, suplantación, divulgación y/o cualquier otro) o incidente informático sobre los recursos TIC institucionales, indicando como mínimo situación, fecha y hora del evento.

4. Respetar y aplicar de manera individual y colectiva los controles de seguridad informática dispuestos por la Universidad para proteger sus recursos informáticos y su información, para lo cual, el Departamento de Tecnología Informática y Comunicaciones tiene la autonomía, con o sin previo aviso, de monitorear, investigar, interceptar, acceder, escanear, inspeccionar, grabar, bloquear, informar a las autoridades u otras acciones que consideren necesarias sobre estos recursos con el fin de preservar, proteger y promover la confidencialidad, integridad y disponibilidad de la información que se almacena o transita en ellos.

5. Cumplir con la normativa interna, externa y legal vigente, haciendo énfasis en aquellas que regulan la protección de la información y de los datos (Ley 1273 de 2009), la protección de datos personales (Ley 1581 de 2012), la propiedad intelectual (Ley 23 de 1982, Ley 1915 de 2018) y las que modifican, complementan, adicionan y/o cualquier otra relacionada con el uso y protección de las tecnologías informáticas y la información.

Los usuarios administrativos, profesores, estudiantes y egresados de los recursos informáticos de la Universidad deben abstenerse de:

1. Realizar acciones que puedan atentar contra la confidencialidad, integridad y disponibilidad de los recursos informáticos y su información, tales como:

    a. Acceso no autorizado a los recursos informáticos institucionales.

    b. Interrupción u obstrucción no autorizada del funcionamiento de los recursos informáticos.

    c. Interceptación de la información que transmite y/o almacena los recursos informáticos.

    d. Alteración, destrucción o supresión no autorizada de los recursos informáticos y su información.

2. Modificar o alterar las configuraciones, propiedades, metadatos, logs u otro tipo de información de auditoría y seguridad de los recursos informáticos.

3. Usar desproporcionadamente los recursos informáticos de manera tal que se niegue a otros usuarios el acceso razonable a estos recursos o que aumente sustancialmente los costos de los recursos tecnológicos.

4. Obstaculizar el desarrollo de las actividades de gestión, revisión y monitoreo de los recursos informáticos por parte Departamento de Tecnología Informática y Comunicaciones.

CAPÍTULO 2. Correo Electrónico Institucional de la Universidad

Los usuarios de la comunidad rosarista que tengan asignado correo electrónico institucional deben:

1. Emplear el correo electrónico únicamente para los fines institucionales pertinentes, siendo responsabilidad del usuario su uso adecuado, seguro y eficiente.

2. Proteger la información almacenada en los buzones de correo mediante le cuidado, reserva y adecuado uso del acceso al correo.

3. La información almacenada en el correo electrónico institucional es propiedad de la Universidad, salvo excepciones contractuales e información personal que sea reportada como tal. Para los casos en que la cuenta de correo comparte roles de -egresado o estudiante- con roles de -administrativos, profesores y contratistas, la información contenida en los buzones de correo es propiedad de la Universidad hasta el momento de la desvinculación laboral, momento en el cual la Universidad procede previa solicitud del jefe inmediato a través de la herramienta gestión de servicios 2030 para la realización de la copia de seguridad del buzón de correo.

4. Realizar tratamiento confidencial a las claves de acceso otorgadas para el uso del correo electrónico.

5. Gestionar periódicamente el consumo de almacenamiento de los buzones de correo, con el fin de reducir los riesgos de seguridad informática el cual genera un riesgo de sufrir una vulneración de datos.

6. Tener especial precaución en el momento de registrar los destinatarios de los correos electrónicos, especialmente cuando la información remitida es de carácter confidencial, privada o sensible. Es responsabilidad del usuario que la información remitida sea enviada a los destinatarios autorizados para su uso.

7. Todo usuario que identifique el recibo de un correo sospechoso, spam o con características malintencionadas, por favor reportarlo a Servicios 2030 y eliminarlo inmediatamente.

Los usuarios del correo electrónico deben abstenerse de:

1. Hacer uso del correo electrónico para fines diferentes a los institucionales.

2. Hacer uso del correo para difundir información falsa, engañosa, ofensiva, discriminatoria o ilícita.

3. Registrar las cuentas de correo institucionales en sitios web de uso personal o sitios no confiables.

4. Descargar archivos o abrir los enlaces contenidos en los mensajes de los correos enviados por remitentes desconocidos o no confiables.

5. Manipular mensajes y archivos que contengan malware o que atenten contra la propiedad intelectual.

CAPÍTULO 3. Servicio de Red de Datos e Internet de la Universidad

Los usuarios de servicio de red de datos e internet deben abstenerse de:

1. Acceder a páginas web no confiables o relacionadas con explotación de vulnerabilidades informáticas, distribución de software malicioso (malware), sitios de descarga de archivos (ej. BitTorrent, emule), sitios web para suplantación de identidad (phishing) o cualquier otra página que pueda generar riesgos informáticos.

2. Abstenerse de conectar dispositivos de computo a los puntos de la red de datos, en oficinas, salas de cómputo, laboratorios, puntos de acceso a WIFI, zonas comunes, etc., sin previa autorización y/o reporte a la Dirección de Tecnología, Informática y Comunicaciones.

3. Utilizar el servicio de red e internet para enviar, intercambiar y/o publicar mensajes con información falsa, engañosa, ofensiva, discriminatoria o ilícita.

4. Utilizar el servicio de red e internet para realizar actividades de escaneo, identificación y explotación de vulnerabilidades de seguridad informática dirigidas hacia la red institucional u otras redes externas, salvo las actividades académicas que lo requieran, las cuales deben ser informadas previamente al Departamento de Tecnología Informática y Comunicaciones para tomar las medidas de control necesarias.

CAPÍTULO 4. Equipos de Cómputo Institucionales.

Los usuarios administrativos, profesores y terceros con asignación de equipos de cómputo institucionales deben:

1. Con el fin de garantizar la protección y respaldo de la información institucional, especialmente aquella que se encuentra almacenada en los equipos de cómputo institucionales, es responsabilidad del usuario salvaguardar esta información a través de los diferentes servicios y plataformas tecnológicas disponibles para almacenar la información en los repositorios suministrados por la Universidad, tales como OneDrive o SharePoint Institucional, servicio de backup de usuarios finales, servicio institucional de carpetas compartidas. Para tal efecto toda la información

institucional es propiedad de la Universidad y debe velar por su confidencialidad, integridad y disponibilidad.

2. Bloquear la sesión en los equipos de cómputo al momento de retirarse temporalmente del puesto de trabajo.

3. Los usuarios en trabajo remoto deben cumplir con las políticas establecidas en el **"Manual - política de seguridad de la información para teletrabajo"** y las **"Políticas del programa de teletrabajo"**; disponibles en el link de acceso inserto en cada título URosario Cowork; en la sección "Generalidades Teletrabajo"; "Cuales documentos harán parte íntegra del Otrosí".

   Los usuarios administrativos, profesores y terceros con asignación de equipos de cómputo institucionales deben abstenerse de:

   1. Dejar encendidos los equipos de cómputo en horas no laborables, excepto en los casos que sea requerido para trabajo con escritorios remotos autorizados y que no representen vulneración a la información institucional.

   2. Dejar los equipos de cómputo desatendidos en lugares públicos o a la vista, en los casos en que estén siendo transportados, para evitar en caso de siniestros riesgos de la información institucional.

   3. Interrumpir las actualizaciones y parches de seguridad que se estén ejecutando en los equipos de cómputo, y es su deber permitir los reinicios cuando las aplicaciones lo soliciten.

   4. Interrumpir los escaneos automáticos para análisis de Malware (ej. virus informáticos, Spyware).

   5. Descargar, instalar y/o usar programas no autorizados, de uso personal o que violen la propiedad intelectual en los equipos de cómputo asignados. Para el caso de los usuarios que cuentan con privilegios de administrador del equipo es su responsabilidad cumplir con los derechos de propiedad intelectual. Esta autorización de usuario administrador es suministrada por el Departamento de Tecnología Informática y Comunicaciones previa solicitud de acuerdo con el Procedimiento: Asignación de Permisos de Administrador en Equipos Institucionales.

   6. Instalar y/o usar programas de acceso remoto para ingresar desde o hacia los equipos de cómputo. No obstante, la Universidad dispone de las herramientas autorizadas para tal fin en caso de requerirse previa autorización del Departamento de tecnología, Informática y Comunicaciones.

   7. Instalar y/o usar programas de sincronización, carga y alojamiento de archivos en internet, excepto el servicio institucional OneDrive suministrado a través de Microsoft Office 365 u otros servicios autorizados previamente por el Departamento de Tecnología Informática y Comunicaciones, para evitar pérdidas de información.

8. Utilizar medios de almacenamiento externos (ej. discos duros externos, USB) en los equipos de cómputo. Salvo autorización previa del Departamento de Tecnología Informática y Comunicaciones.

CAPÍTULO 5. Equipos de Cómputo NO Institucionales.

Los usuarios administrativos, profesores y terceros con equipos de cómputo no institucionales deben:

1. Contar con los sistemas operativos y antivirus actualizados en los equipos de cómputo personales en caso de que estos sean conectados a la red de datos cableada o inalámbrica institucional. Es responsabilidad del usuario tomar las precauciones de seguridad necesarias en sus equipos y responder por los incidentes de seguridad informática causados por ellos.

2. El mantenimiento correctivo y preventivo se realiza únicamente a los equipos y el software que son propiedad de la Universidad del Rosario.

3. Las atenciones de las solicitudes de servicio se realizan únicamente a los recursos e inventario que sean propiedad de la Universidad.

V. GLOSARIO:

- **Recursos Informáticos:** Medios tecnológicos que habilitan y facilitan el desarrollo de las actividades y labores en la Universidad del Rosario, tales como: equipos de cómputo, dispositivos informáticos, aplicaciones, sistemas de información, servidores, red de datos y comunicaciones, internet, correo electrónico, soluciones de colaboración y ofimática, servicio institucional de carpetas compartidas (Urfiles), servicio de backup, entre otros.
- **Usuario:** Persona que pertenece a la comunidad rosarista e invitados institucionales.
- **Confidencialidad:** La información no debe ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. [ISO 27001]
- **Integridad:** Es deber de la Universidad el mantenimiento de la exactitud y completitud de la información.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. [ISO 27001]
- **Activo de Información**: Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos

de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, entre otros[1].

- **Antivirus:** Programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso, así como proteger los equipos de otros programas peligrosos conocidos genéricamente como malware[2].
- **Incidente de Seguridad**: Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información[3].
- **Malware**: Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información.
- **Parche de Seguridad**: Es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del software tras la detección de una vulnerabilidad en el software y pueden instalarse de forma automática o manual por parte del usuario.
- **Phishing**: Técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.
- **Metadatos**: Los metadatos son el conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión. Los metadatos es una información que enriquece el documento al que está asociado.
- **Spam**: Es el correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva.
- **Spyware**: Es un malware que recopila información de un ordenador y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del ordenador.
- **Suplantación de Identidad**: Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude o acoso.
- **Vulnerabilidad**: Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota.

[1] GLOSARIO DE TÉRMINOS DE CIBERSEGURIDAD. Una guía de aproximación para el empresario. Instituto Nacional de Ciberseguridad. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf
[2] GLOSARIO DE TÉRMINOS DE CIBERSEGURIDAD. Una guía de aproximación para el empresario. Instituto Nacional de Ciberseguridad. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf
[3] GLOSARIO DE TÉRMINOS DE CIBERSEGURIDAD. Una guía de aproximación para el empresario. Instituto Nacional de Ciberseguridad. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

VI. COMUNICACIONES

Toda notificación, reporte, autorización, inquietud o solicitud de información relacionada a las políticas de seguridad informática presentadas en este documento, se debe realizar al Departamento de Tecnología Informática y Comunicaciones a través Servicios 2030 por el correo electrónico: servicios2030@urosario.edu.co, por la extensión 2030 y/o por los canales que se establezcan para el efecto.

VII. VIGENCIA

La presente Circular Normativa deroga la Circular Normativa 110 SIND 2020- Políticas de Seguridad Informática y rige a partir de la fecha de su emisión.

ANA ISABEL GÓMEZ CÓRDOBA
Rectora

ELABORÓ/MODIFICÓ	REVISÓ Y APROBÓ
LILIA XIMENA CARDOZO CARRASCO Coordinador de Telecomunicaciones y Ciberseguridad Dirección de Tecnología, Informática y Comunicaciones Fecha: Noviembre de 2024 **JAIRO NAYIB SANTOS GÓMEZ** Coordinador Servicios e Infraestructura Dirección de Tecnología, Informática y Comunicaciones Fecha: Noviembre de 2024 **DALHIA MILENA CARDENAS BERMUDEZ** Analista de Gobierno y Calidad Dirección de Tecnología, Informática y Comunicaciones Fecha: Noviembre de 2024	**JORGE ENRIQUE MOLINA ZAMBRANO** Director Dirección de Tecnología, Informática y Comunicaciones Fecha: Noviembre de 2024 **LUCY ARIARI CORTÉS TRUJILLO** Directora Dirección Financiera Fecha: Noviembre 2024 **XIMENA BETANCOURT DE CASTRO** Directora Dirección Jurídica Fecha: Noviembre de 2024 **GERMAN VILLEGAS GONZALEZ** Secretario General Fecha: Noviembre de 2024

Proceso de firma electrónica Neon v2

ELABORÓ **JUANITA HINCAPIÉ RESTREPO** PROFESIONAL JURIDICO *21-11-2024 09:58:03*
REVISÓ **ANGELA VIVIANA BECERRA ROJAS** ANALISTA DE TRANSFORMACIÓN ORGANIZACIONAL *21-11-2024 12:41:28*
APROBÓ **JORGE ENRIQUE MOLINA ZAMBRANO** DIRECTOR DIRECTOR DE TECNOLOGÍA INFORMÁTICA Y COMUNICACIONES *21-11-2024 13:06:08*
APROBÓ **LUCY ARIARI CORTÉS** DIRECTOR FINANCIERO *16-01-2025 14:57:53*
APROBÓ **XIMENA BETANCOURT DE CASTRO** DIRECTOR JURIDICO *17-01-2025 08:11:29*
APROBÓ **GERMAN VILLEGAS GONZALEZ** SECRETARIO GENERAL *17-01-2025 13:35:57*