

	PROCESO GESTION TECNOLÓGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	VERSIÓN: 01
		FECHA: 16/12/2021

TABLA DE CONTENIDO

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO	VERSIÓN: 01
	ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	FECHA: 16/12/2021

1. INTRODUCCION

Este documento hace parte de las Políticas Generales de Seguridad de la Información definidas por el Instituto de la juventud, el deporte y la recreación de Bucaramanga y por tanto es el núcleo principal del Modelo de Seguridad para la protección de la información en la Entidad.

Las políticas expresadas en este manual son la base para la implantación de normas y procedimientos, para dar la posibilidad de construir una arquitectura de seguridad sustentada en procesos homogéneos y estándares, integrada con la arquitectura de tecnología informática y con un ambiente de administración y control efectivo, que garanticen la seguridad de la información en el Instituto.

La implantación de nuevas herramientas de Hardware y Software, de Sistemas de Información y de otros recursos de información deben cumplir con las políticas definidas en este manual, con el propósito de que el Modelo de Seguridad de la Información se mantenga actualizado en forma dinámica, ya que su objeto es la protección de la información.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	VERSIÓN: 01
		FECHA: 16/12/2021

2. JUSTIFICACION

En la actualidad en los sectores públicos, privados y académicos, basan gran parte de su desarrollo y el que hacer de sus labores en sistemas informáticos. Esto hace necesario que cada vez se preste mayor atención a la disponibilidad, confidencialidad e integridad de la información, garantizando la continua prestación de sus servicios, así como la certeza de tener su información segura y sus sistemas protegidos.

Las políticas se establecen para sensibilizar a los usuarios de los riesgos asociados con el uso de los recursos tecnológicos (equipos) y servicios de red que estén a disposición de los funcionarios del el Instituto de la juventud, el deporte y la recreación de Bucaramanga. Debido a que las acciones contrarias a las políticas señaladas pueden traer consecuencias de tipo legal, administrativas, económicas, daños físicos, tanto al INDERBU como al usuario o al equipo de cómputo.

Todos los usuarios están obligados de acatar los lineamientos plasmados en la presente política, con el fin de realizar sus operaciones diarias minimizando el riesgo de llevar a cabo el uso inadecuado o prácticas impropias en dichos recursos.

Con base en lo anterior, se hace necesario contar con estrategias y medidas de seguridad de la información, para garantizar el funcionamiento adecuado de todos los sistemas y para que, en un momento dado, se puedan aplicar los correctivos necesarios en caso de un eventual ataque o desastre que impliquen la pérdida de la información y los sistemas informáticos.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO	VERSIÓN: 01
	ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	FECHA: 16/12/2021

3. MARCO NORMATIVO

Con el transcurrir del tiempo se han desarrollado diferentes estándares relacionados y que van en pro de la seguridad de la información indiferente al tamaño o enfoque en el que se desempeñen las empresas y organizaciones.

ISO 27001: ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

ISO 27002: La norma ISO 27002 (anteriormente denominada ISO 17799) es un estándar para la seguridad de la información que ha publicado la organización internacional de normalización y la comisión electrotécnica internacional.

La versión más reciente de la norma ISO 27002:2013. La norma ISO 27002 proporciona diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información.

La seguridad de la información se define en el estándar como “la preservación de la confidencialidad, integridad y disponibilidad. Para saber más sobre los demás dominios puede leer La norma ISO 27002 complemento para la ISO 27001.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	VERSIÓN: 01
		FECHA: 16/12/2021

4. OBJETIVO

Establecer las responsabilidades y lineamientos mínimos que deben cumplir todos los usuarios del correo institucional con el fin de garantizar el correcto uso del mismo, y asegurar un mejor aprovechamiento del correo como una herramienta de trabajo que provee el INDERBU para beneficio de cada uno de sus funcionarios y contratistas.

5. ALCANCE

Esta política aplica a todos los usuarios que conforman el Instituto de la juventud, el deporte y la recreación de Bucaramanga (funcionarios de planta y contratistas) y busca establecer los lineamientos, responsabilidades, normas y buenas prácticas que aplican para el uso adecuado del correo institucional del Instituto.

6. RESPONSABLES

Subdirección Administrativa y Financiera – Apoyo Tecnológico y de Información

- Elaboración y actualización de la presente Política.
- Evaluación del cumplimiento de la presente Política.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO	VERSIÓN: 01
	ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	FECHA: 16/12/2021

7. DESARROLLO

El correo electrónico institucional es un medio formal y oficial de comunicaciones del INDERBU y una herramienta de trabajo que se ha dispuesto con el fin de facilitar las labores propias de los cargos de cada uno de sus funcionarios de planta y contratistas; teniendo en cuenta esto, es primordial establecer los lineamientos que se deben tener presente de acuerdo con las obligaciones y prohibiciones que cada funcionario debe tener presente.

El Instituto puede implementar las medidas necesarias en la plataforma del correo institucional, en aras de incrementar los niveles de seguridad y/o de brindar un mejor servicio.

El cumplimiento de las políticas plasmadas en el presente documento en ningún momento reemplaza las políticas de seguridad, privacidad y uso del correo establecidas por “Gmail o OUTLOOK” el desarrollo de la presente política está pensada en fomentar responsabilidad, respeto, integridad y la seguridad de la información.

El Instituto de la juventud , el deporte y la recreación de Bucaramanga se reserva el derecho de deshabilitar, modificar o eliminar las cuentas de correo institucional, en las cuales se evidencie un uso inadecuado o que incurran en el incumplimiento de las políticas plasmadas en el presente documento; o que el funcionario ya no trabaje para el INDERBU.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO	VERSIÓN: 01
	ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	FECHA: 16/12/2021

8. RESPONSABILIDADES DE LOS USUARIOS DE LOS CORREOS

- Los usuarios son responsables de todas las actividades que se realicen desde su cuenta de correo institucional.
- La cuenta de correo electrónico es de uso personal e intransferible. El usuario (funcionario o contratista del INDERBU) se compromete a hacer un uso responsable de la cuenta y a mantener su contraseña en secreto, cambiarla periódicamente y no prestarla bajo ninguna circunstancia; así mismo, el usuario se compromete a notificar al administrador del correo electrónico de manera inmediata la pérdida de su contraseña o el acceso no autorizado por parte de terceros a su cuenta.
- Es responsabilidad de los usuarios (funcionario o contratista del INDERBU) utilizar el sistema de correo electrónico de la institución, exclusivamente para asuntos relacionados con sus labores, por lo tanto, el usuario debe hacer uso de este servicio implementando criterios de racionalidad, respeto, responsabilidad, integridad y seguridad de la información.
- Asegurarse que los mensajes no contengan comentarios abusivos, obscenos, difamatorios, ni material alguno que pueda poner en situación conflictiva a la institución y al funcionario.
- Informar a su supervisor o jefe inmediato, en caso de recibir mensajes como los descritos en el párrafo anterior que puedan interpretarse como ofensivos y posteriormente eliminarlos.
- Es responsabilidad del usuario (funcionario o contratista del INDERBU) realizar copias de seguridad o solicitar las copias de seguridad del archivo que almacena la información contenida en el correo y de la libreta de direcciones.
- El envío de correos electrónicos implica el consumo de recursos tecnológicos y demanda tiempo a la persona receptora, por tal razón se debe evitar el envío de correos innecesarios y que no guarden relación con el desempeño de las funciones asignadas. Antes de responder o reenviar un correo, el usuario debe validar si se requiere incluir todos los destinatarios, el historial y la información que posee el mismo.
- Todo correo de procedencia desconocida, correo basura, SPAM, correo no deseado, etc. que sea recibido en los buzones de correo electrónico del Instituto, debe ser ignorado, eliminado inmediatamente con el fin de evitar posibles infecciones por código malicioso o virus.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO	VERSIÓN: 01
	ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	FECHA: 16/12/2021

- El usuario (funcionario o contratista del INDERRBU) del correo electrónico se compromete a reportar oportunamente a la Subdirección Administrativa y Financiera – Apoyo Tecnológico y de Información, cualquier fallo de seguridad de su cuenta institucional, incluyendo el uso no autorizado, pérdida de contraseñas, etc.
- El correo electrónico institucional es una herramienta de trabajo, de uso exclusivamente laboral, por tanto, la información contenida en estos es de propiedad de la Entidad. En esa medida, el Instituto de la juventud , el deporte y la recreación de Bucaramanga no se hace responsable de la información de carácter personal que los usuarios almacenen en las cuentas institucionales.
- En caso de que se requiera el funcionamiento de una sola cuenta de correo para dos o más usuarios, el usuario principal y dueño de la cuenta de correo debe otorgar dicha autorización por escrito o por correo electrónico indicando que usuarios tendrán acceso a la cuenta de correo, y en todo caso dicha autorización no exime de toda responsabilidad al usuario dueño de la cuenta del correo, uso de la cuenta y de los lineamientos planteados en el presente documento.
- El INDERBU recomienda hacer caso omiso a los links que vengan agregados en el cuerpo del correo de cuentas externas y de dudosa procedencia; por lo tanto, se aconseja digitar directamente la página que deseen consultar en el navegador de internet de su computador, esto para evitar que dentro del link que se anexa en el correo de dudosa procedencia estén ocultos links que pueden capturar información de la cuenta de correo, del Sistema Operativo, de las transacciones electrónicas y encriptar la información almacenada en el disco duro ocasionando pérdidas económicas y daños irreversibles en la información.
- No enviar ni contestar cadenas de correo o cualquier otro esquema de "pirámide" de mensajes.
- Asignar una contraseña mínima de 8 caracteres con grado de dificultad alto.
- Acceder solo desde computadoras confiables: Algunas computadoras que se encuentran en sitios públicos (café internet) podrían tener instalado algún programa que rastree las pulsaciones de teclas y podrían apropiarse de las contraseñas.
- Cerrar sesión cada vez que deje de usar el correo electrónico; es recomendable cerrar sesión cada vez que haya enviado o leído algún correo electrónico o cuando se retire del puesto de trabajo. Cualquier persona podría cambiar los accesos a tu cuenta o utilizar tu correo con fines criminales.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO	VERSIÓN: 01
	ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	FECHA: 16/12/2021

9. RESTRICCIONES EN EL USO DEL CORREO INSTITUCIONAL

- El envío de correos con mensajes que contravengan las normas legales, la moral, el orden público, la intimidad o el buen nombre de las personas, que contengan contenido irrespetuoso, difamatorio, racista, religioso, irrespetuoso, discriminatorio, de acoso o intimidación; así como imágenes o videos con contenidos ilegales, ofensivo, extorsivo, indecente o con material sexual.
- Al ser el correo electrónico institucional la herramienta dispuesta por el Instituto como medio de comunicación oficial, se prohíbe el uso de correos personales con el fin de establecer o transferir información institucional.
- Copiar o reenviar correos electrónicos que se encuentren clasificados como CLASIFICADOS o SECRETOS en el asunto del mensaje, sin tener la autorización del remitente original para hacerlo.
- Usar el correo electrónico institucional para el envío de propaganda, ofertas, negocios personales, avisos publicitarios o cualquier información ajena a las laborales propias del cargo.
- La propagación de correos de procedencia desconocida, SPAM, correo basura o no deseado, hacia cuentas institucionales

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO	VERSIÓN: 01
	ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	FECHA: 16/12/2021

10. CAMBIO PERIODICO DE LA CONTRASEÑA

El uso de contraseña es un aspecto fundamental de la seguridad de los recursos informáticos; una contraseña mal elegida puede generar problemas de seguridad en la organización. El objetivo fundamental de este documento es establecer un estándar para la creación de contraseñas fuertes, favorecer su protección, así como el cambio frecuente de las mismas. El ámbito de estas recomendaciones incluye a todos aquellos usuarios de los servicios y recursos informáticos del Instituto de la juventud, el deporte y la recreación de Bucaramanga que tienen o son responsables de una cuenta (o cualquier otro tipo de acceso que requiera contraseña) en cualquiera de los sistemas del Instituto.

Esto ayuda a que no rastreen tu contraseña y si alguien pudo obtenerlo. Si te das cuenta que alguien ha estado enviando correo electrónico desde tu cuenta, es recomendable cambiar la contraseña lo antes posible.

Crear una contraseña segura es un componente importante en la protección de su cuenta de correo corporativo. Una contraseña segura nos permite proteger su información personal, proteger tus correos electrónicos, archivos y demás contenido y evitar que otra persona acceda a tu cuenta sin autorización.

La contraseña del correo electrónico es personal e intransferible, el uso irresponsable de estas puede ocasionar suplantaciones de la identidad del correo y ser utilizado por otros para generar ataques a sitios web y envío de correos electrónicos. Se recomienda realizar el cambio de este mínimo una vez cada dos meses si no se observa movimientos inadecuados en su cuenta.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	VERSIÓN: 01
		FECHA: 16/12/2021

Los parámetros para asignar la contraseña al correo corporativo @inderbu.gov.co son los siguientes.

11. GESTION DE CONTRASEÑAS SEGURAS

- Se deben combinar números, letras mayúsculas y minúsculas y símbolos.
- No se deben usar secuencias de números ni caracteres repetitivos.
- La contraseña no debe estar asociada al ID de inicio de sesión, nombre, fecha de nacimiento, teléfonos, número de cédula o datos de familiares.
- Se debe evitar la participación de terceros y el uso de mensajes de correo electrónico sin protección, en el proceso de entrega de la contraseña a los usuarios.
- Las contraseñas pueden incluir cualquier combinación de caracteres ASCII imprimibles (no se aceptan caracteres especiales como la ñ o acentos).
- Deben tener mínimo 8 caracteres.
- Las contraseñas no pueden empezar ni terminar con un carácter de espacio en blanco.
- Ejemplo de una contraseña segura: F3l1zN@v1d@D

Nota: Ver política de uso de contraseñas del INDERBU.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO	VERSIÓN: 01
	ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	FECHA: 16/12/2021

12. INTERCAMBIO ELECTRONICO DE INFORMACION

Es la transmisión estructurada de datos entre organizaciones por medios electrónicos. Se usa para transferir documentos electrónicos o datos de negocios de un sistema computacional a otro. Este intercambio puede realizarse en distintos formatos: EDIFACT, XML, ANSI ASC X12, TXT, etc. Por tanto, se recomienda lo siguiente:

- Proteger los datos intercambiados de la interceptación, copia, modificación, enrutamiento y destrucción.
- Proteger información sensible que se encuentre en forma de archivo adjunto.
- Usar técnicas criptográficas para proteger la confidencialidad, integridad y autenticidad de la información.

13. ENVIO DE CORREOS MASIVOS ,CORREOS ELECTRONICOS

Para el envío de correos masivos, comunicados, etc., y en caso que alguna área, departamento o funcionario requiera enviar algún correo masivo al personal del Instituto o ciudadanos que tengan algún trámite con el Instituto de la juventud , el deporte y la recreación de Bucaramanga, deberá solicitarlo a la Oficina de la Subdirección Administrativa y Financiera - Apoyo Tecnológico y de Información, quienes evaluarán la pertinencia o no de dicha solicitud y realizará las actividades técnicas en la plataforma del correo electrónico.

Se recomienda en los casos que se requiera el envío de correos masivos que los contactos de los destinatarios se agreguen en la opción de copia oculta con el objetivo de proteger la dirección de cada destinatario.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO	VERSIÓN: 01
	ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	FECHA: 16/12/2021

14. CADUCIDAD DE LA CUENTA DE CORREO ELECTRONICO.

La desactivación de una cuenta de correo electrónico supone la pérdida automática de la capacidad de enviar y recibir mensajes.

- Como norma general, las cuentas de correo electrónico se mantendrán activas mientras la relación de la persona con la Institución esté vigente.
- La desactivación del correo se realizará cuando un servidor público sea separado de la institución y previa notificación por parte de la Dirección de Talento Humano o el Supervisor del contrato, quienes reportaran a la Oficina de la Subdirección Administrativa y Financiera - Apoyo Tecnológico y de Información.
- Una vez cesada esta relación (jubilación, finalización de contrato, etc.) las cuentas serán eliminadas en el plazo de 15 días o renombradas al nuevo funcionario.
- Cuando un funcionario no continúa laborando con el Instituto, deberá proporcionar la información de la cuenta asociada al funcionario que lo suceda o hacer entrega de la cuenta al jefe inmediato o supervisor del contrato, para reasignar la cuenta de correo electrónico al nuevo funcionario o proceder a realizar copia de seguridad y eliminación de la cuenta electrónica.

15. CRITERIOS DE AUTORIZACION

La creación de usuario debe ser solicitada por la Oficina de Recurso Humano, en caso de ser contratista este debe ser requerido por el supervisor del contrato, vía correo electrónico, con especificación de la necesidad (correo electrónico). Esta solicitud deberá ser aprobada por la Subdirección Administrativa y Financiera.

	PROCESO GESTION TECNOLOGICA	CÓDIGO: PA.05-PO1
	POLÍTICA DE USO DE CORREO ELECTRONICO ASOCIADA A LA POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	VERSIÓN: 01
		FECHA: 16/12/2021

16. POLITICA DE TRATAMIENTO DE DATOS PERSONALES.

Aviso de Confidencialidad de Correo Electrónico, se asigna en todos los correos corporativos en el pie de página, estableciendo el procedimiento del uso del contenido del correo y la información adjunta.

“La información de este mensaje es legalmente privilegiada y para uso exclusivo del destinatario. Su reproducción, uso, interceptación, retención o sustracción, está prohibida a personas diferentes al destinatario, acciones que serán penalizadas conforme las normas legales vigentes. Si ha recibido este correo por equivocación u omisión, por favor notifique de inmediato al remitente y destruya la información aquí contenida.

Remitir sus datos personales por medio de este correo electrónico configura una conducta inequívoca que autoriza el tratamiento de los mismos conforme a la Política de Tratamiento de la Información del instituto de la juventud el deporte y la recreación de Bucaramanga, que incluye los canales de atención para ejercer sus derechos como titular y que puede consultar en nuestra página web”

17. CONTROL DE CAMBIOS.

FECHA	VERSION	DETALLE DEL CAMBIO
23/04/2023	Versión 1.	Elaboración de la política

Elaboro

Ing. William Oswaldo Barrera

Ing. Mónica Niño