Tabla de contenido

1. OBJETIVOS.

1.1.1 Objetivo General

Establecer un marco normativo que oriente la protección de la información institucional en la SERCOP, mediante la implementación de políticas de seguridad alineadas a las buenas prácticas y estándares internacionales vigentes, conforme a la legislación aplicable actual con el fin de garantizar y preservar la información institucional tomando en cuenta los principios de confidencialidad, integridad y disponibilidad.

1.1.2 Objetivo Específicos

- Definir las directrices que orienten el uso, manejo, protección y control de la información en todos los niveles de la institución.
- Establecer de manera precisa las responsabilidades para los funcionarios, contratistas y terceros que interactúan con los activos de información.
- Fomentar una cultura organizacional orientada a la seguridad de la información, a través de sensibilización, formación continua y el cumplimiento de las políticas establecidas.
- Asegurar la implementación de controles y acciones, tanto preventivas como correctivas que permitan gestionar de manera efectiva los riesgos asociados a la seguridad de la información.

2. ALCANCE.

Las políticas de seguridad de la información definidas en el presente documento son de aplicación y cumplimiento obligatorio para todo personal de SERCOP y terceras partes debidamente autorizadas que gestionan, acceden, procesan, almacenan o transmiten información de la institución para el cumplimiento de sus funciones, conforme a los procedimientos establecidos y en apego a los instrumentos legales aplicables.

3. BASE LEGAL.

- Registro oficial Acuerdo Ministerial No. 0003-2024-EGSI-versión-3.0
- EL ESTATUTO ORGÁNICO DE GESTIÓN ORGANIZACIONAL POR PROCESOS DEL SERVICIO NACIONAL DE CONTRATACIÓN PÚBLICA – SERCOP, RESOLUCIÓN DSERCOP-0013-2017.
- Ley Orgánica de Protección de Datos Personales publicada en el Suplemento del Registro Oficial No. 459 del 26 de mayo de 2021

4. RESPONSABILIDADES.

4.1. Comité de Seguridad de la Información de SERCOP

1. Preparar y gestionar la aprobación de la política y disposiciones normativas institucionales en materia de seguridad de la información, por parte de la máxima autoridad del SERCOP.
2. Evaluar y dar seguimiento al proceso de identificación, análisis y tratamiento de riesgos relacionados con la información, priorizando acciones preventivas y correctivas.
3. Colaborar con la gestión de incidentes de seguridad relevantes, asegurando una respuesta oportuna y coordinada, así como la revisión posterior para evitar recurrencias.
4. Monitorear el despliegue y funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI), verificando que se apliquen controles eficaces para proteger los activos de la información.
5. Promover el conocimiento y formación del personal en buenas prácticas de seguridad de la información, iniciando un entorno institucional donde se valore y proteja la información.
6. Revisar y garantizar los planes de continuidad del negocio y recuperación ante desastres desde la perspectiva de la seguridad de la información, verificando que contemplen salvaguardas adecuadas.

7. Revisar y validar la política de seguridad, junto con sus revisiones y actualizaciones, asegurando que se mantenga alineada con los objetivos estratégicos de la institución.
8. Informar a la máxima autoridad los avances de la implementación del EGSI.
9. Reportar a la máxima autoridad las alertas que impidan la implementación del EGSI.
10. Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del EGSI.
11. Velar por la aplicación de las Normas Técnicas Ecuatorianas INEN/ISO/IEC 27000 para la Gestión de Seguridad de la Información.
12. Designar formalmente a un servidor como Oficial de Seguridad de la Información, en base al perfil establecido.
13. Designar a los custodios o responsables de la información de las diferentes áreas de la entidad
14. Prepara y gestionar la aprobación del Informe de Cumplimiento de la Gestión de Riesgos, por parte de la máxima autoridad del SERCOP, el cual será remitido hasta el 31 de enero de cada año a la Subsecretaría de Estado – Gobierno Electrónico del Ministerio de Telecomunicaciones y Sociedad de la Información.
15. Las demás que determine el Comité previa autorización de la máxima autoridad institucional, necesarias para la implementación, control y seguimiento del EGSI.
16. Impulsar el ciclo Plan-Do-Check-Act (PDCA), para garantizar que la seguridad de la información se desarrolle conforme a las necesidades del negocio y las amenazas emergentes.
17. Asegurar que los temas tratados en el comité se manejen con la debida confidencialidad, evitando filtraciones o mal uso de información sensible.

4.2. Oficial de Seguridad de la Información

1. Identificar todas las personas o instituciones públicas o privadas, que de alguna forma influyen o impactan en la implementación del EGSI.
2. Estructurar, documentar y mantener actualizado las Políticas de Seguridad de la Información, asegurando que estas estén alineadas con el marco legal vigente y los objetivos estratégicos de la institución.
3. Asesorar, en coordinación con la Dirección de Comunicación y la Dirección de Administración de Recursos Humanos, a los servidores en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas.
4. Desarrollar campañas, capacitaciones y actividades que fortalezcan la cultura de seguridad entre los servidores y fomenten comportamientos responsables.
5. Elaborar un plan de seguimiento y control de la implementación de las medidas de mejora o acciones correctivas.
6. Coordinar la elaboración del Plan de Continuidad de Seguridad de la Información.
7. Orientar y generar un procedimiento adecuado para el manejo de los incidentes de seguridad de la información presentados al interior del SERCOP, desde su detección hasta su resolución, incluyendo la evaluación de la causa principal y la definición de medidas correctivas.
8. Coordinar la gestión de incidentes de seguridad con nivel de impacto alto a través de otras instituciones gubernamentales.
9. Mantener al día los procedimientos, instructivos y registros relacionados con la seguridad, garantizando que estén accesibles, actualizados y controlados.
10. Verificar el cumplimiento de las disposiciones normativas, procedimientos y controles de seguridad institucionales establecidos.
11. Informar al Comité de Seguridad de la Información, el avance de la implementación del EGSI, así como las alertas que lo impidan.
12. Transferir la documentación e información de su gestión, al nuevo Oficial de Seguridad, previa la terminación de sus funciones; o, en caso de ausencia, al Comité de Seguridad de la Información
13. Mantenerse informado sobre amenazas emergentes, vulnerabilidades y nuevas tecnologías, proponiendo mejoras o controles adicionales cuando sea necesario.

14. Asegurar que se identifiquen, clasifiquen y protejan adecuadamente todos los activos de información críticos para la organización.
15. Actuar como contraparte del Ministerio de Telecomunicaciones y de la Sociedad de la Información en la actualización e implementación del EGSI, quienes reportarán a través del sistema Gobierno por Resultados (GPR).

4.3. Dirección de Talento Humano

1. Garantizar que la seguridad de la información esté integrada en cada etapa del ciclo de vida del servidor: desde la contratación, pasando por el desarrollo profesional, hasta su salida de la organización.
2. Incluir responsabilidades, competencias y requisitos específicos de seguridad en las descripciones de los cargos, especialmente para puestos críticos o de alto acceso a información sensible.
3. Organizar para que todos los nuevos servidores o ya vinculados, firmen los Acuerdos de confidencialidad conjuntamente con el Oficial de Seguridad de la Información de manera periódica.
4. Ejecutar la firma de cláusulas o acuerdos de confidencialidad, uso aceptable de la información y cumplimiento de políticas por parte del personal y contratistas.
5. Coordinar programas de formación y sensibilización en seguridad de la información para todo el personal, asegurando que comprendan sus responsabilidades y buenas prácticas.
6. Promover valores institucionales que refuercen el compromiso con la protección de la información y el comportamiento ético en el uso de recursos informáticos.
7. Participar en la definición y aplicación de acciones disciplinarias en caso de incumplimientos a las políticas de seguridad, garantizando que se realicen de manera justa y conforme a la normativa interna.
8. Coordinar con las demás áreas para asegurar que los cambios de funciones, reasignaciones o desvinculaciones consideren la baja o modificación de accesos y privilegios en los sistemas de información.
9. Apoyar en la identificación de riesgos humanos en el SGSI, como el acceso no autorizado, errores por desconocimiento o amenazas internas y proponer medidas preventivas.
10. Manejar con especial atención los datos personales de los servidores cumpliendo con las políticas de privacidad y seguridad vigentes.
11. Apoyar en las auditorías internas o externas del SGSI cuando involucren procesos relacionados con el personal, asegurando la disponibilidad de información relevante.
12. Integrar criterios de seguridad de la información en los reglamentos internos, manuales de convivencia y demás documentos de gestión del talento humano.
13. Asegurar que exista un plan de sucesión o transferencia de conocimientos en puestos clave relacionados con la seguridad, para reducir riesgos ante salidas inesperadas.

4.4. Coordinación de Tecnologías de la Información y Comunicaciones

1. Asegurar que todos los desarrollos tecnológicos, nuevas soluciones o implementaciones consideren principios de seguridad en las etapas del ciclo de vida desde la etapa de planificación hasta la etapa de mantenimiento.
2. Analizar los riesgos y beneficios de nuevas herramientas o plataformas antes de su adopción, garantizando que cumplan con los requisitos del SGSI y no introduzcan vulnerabilidades.
3. Contribuir de manera activa en la planificación, evaluación y ejecución de cambios tecnológicos, garantizando que estas se realicen de forma controlada y se documenten conforme a los lineamientos del SGSI vigente.
4. Organizar la implementación de soluciones tecnológicas orientadas a fortalecer la seguridad, como cifrado, autenticación multifactorial (MFA), control de accesos y monitoreo de eventos.
5. Diseñar e implementar soluciones innovadoras que respalden la disponibilidad y recuperación de los sistemas de información críticos ante incidentes o fallos técnicos.
6. Proporcionar evidencia y asistencia técnica durante auditorías del SGSI o revisiones internas, facilitando el análisis de cumplimiento en cuanto a infraestructura, software y servicios.

7. Validar que las innovaciones tecnológicas se alineen con las políticas internas de seguridad, arquitectura tecnológica y gobernanza digital de la organización.
8. Participar en el análisis de riesgos asociados a proveedores tecnológicos, revisando sus prácticas de seguridad, niveles de servicio y cumplimiento de requisitos contractuales.
9. Garantizar la administración adecuada de versiones, parches y actualizaciones de software y hardware, minimizando exposiciones a vulnerabilidades conocidas.
10. Asegurar que los activos tecnológicos bajos su gestión están inventariados, clasificados y protegidos conforme a las directrices del SGSI.
11. Proponer iniciativas de mejora que integren innovación con buenas prácticas de seguridad, contribuyendo al fortalecimiento constante del ecosistema digital institucional.
12. Colaborar de manera cercana con el Oficial de Seguridad de la Información, el área de infraestructura, desarrollo y demás actores de la seguridad.
13. Actualizar la documentación técnica relacionada con la arquitectura, soluciones desarrolladas, configuraciones y procesos, asegurando su confidencialidad y trazabilidad.

4.5. Coordinación de Asesoría Jurídica

1. Brindar orientación especializada para asegurar que el SGSI se ajuste a las leyes, reglamentos, políticas nacionales y compromisos contractuales aplicables en materia de seguridad de la información.
2. Examinar y emitir criterios legales sobre políticas, procedimientos y acuerdos relacionados con la seguridad, garantizando que estén redactados conforme al marco jurídico vigente.
3. Participar en el análisis y gestión de incidentes de seguridad que puedan tener implicaciones legales, como filtraciones de datos personales, uso indebido de información o acceso no autorizado.
4. Verificar que los contratos con proveedores, terceros y aliados estratégicos incluyan cláusulas que protejan la información institucional y asignen responsabilidades claras en temas de seguridad. Además se debe garantizar que esta documentación con valor legal o jurídico sea custodiada adecuadamente y que se establezcan tiempo mínimos de retención conforme a la ley.
5. Velar por el cumplimiento de las normativas de protección de datos personales, incluyendo los derechos de los titulares, deberes del responsable del tratamiento y medidas de seguridad requeridas.
6. Diseñar o revisar cláusulas legales que comprometan al personal, contratistas y proveedores al uso adecuado y confidencial de la información a la que acceden.
7. Asesorar en los procesos sancionatorios internos que se deriven de violaciones a las políticas de seguridad de la información, garantizando el debido proceso y la legalidad.
8. Colaborar en auditorías internas y externas del SGSI cuando se requiera interpretar normativas, contratos o responsabilidades legales asociadas al tratamiento de la información.
9. Contribuir a que los reglamentos internos, instructivos y demás documentos institucionales incluyan disposiciones claras sobre la protección de la información y sus consecuencias legales.
10. Promover la sensibilización del personal sobre las implicaciones legales de manejar información institucional, datos personales o sistemas críticos.

4.6. Dirección de Comunicación Social

1. Diseñar y ejecutar estrategias de comunicación que promuevan entre los colaboradores una cultura institucional en temas de seguridad de la información. A partir del desarrollo de materiales de comunicación (boletines, infografías, mensajes internos, video, etc.) que refuercen las buenas prácticas en el manejo seguro de la información.
2. Apoyar en la preparación de mensajes institucionales ante incidentes de seguridad, asegurando una comunicación oportuna, coherente y transparente hacia el público interno y externo, según la criticidad del evento.
3. Trabajar conjuntamente con el Oficial de Seguridad de la Información para definir contenidos claves en campañas de formación, adaptando el mensaje al perfil de audiencia.
4. Verificar que los mensajes públicos o internos no incluyan datos sensibles, confidenciales o estratégicos que puedan comprometer la seguridad de la información institucional.

5. Elaborar planes o guías que definan cómo y quién debe comunicar en caso de incidentes de seguridad que afecten a la institución, con el objetivo de mantener la confianza y controlar el impacto a la reputación institucional.
6. Mantener un registro ordenado y trazable de las comunicaciones oficiales relacionadas con la seguridad de la información, como respaldo institucional y evidencia de cumplimiento.
7. Contribuir con informes, métricas o retroalimentación sobre el impacto y efectividad de las estrategias de comunicación vinculadas al SGSI.

4.7. Personal de SERCOP

1. Conocer y respetar todas las políticas, normativas y procedimientos relacionados con la seguridad de la información definidos por la institución, sin excepción.
2. Usar la información institucional únicamente para propósitos autorizados y relacionados con su rol, evitando cualquier divulgación, modificación o uso indebido.
3. Mantener la confidencialidad sobre datos sensibles, personales o estratégicos, incluso tras la finalización de la prestación de servicios en la institución.
4. Hacer un uso correcto y ético de los sistemas informáticos, redes, correo institucional y demás herramientas digitales, cumpliendo con las normas de uso aceptable.
5. Informar de manera inmediata al Oficial de Seguridad de la Información o el área encargada, en caso de detectar comportamientos sospechosos, errores, accesos indebidos o cualquier incidente que comprometa la seguridad.
6. Participar y comprometerse de manera activa en los programas de formación y sensibilización en seguridad de la información organizados por la institución.
7. Proteger sus usuarios y contraseñas, evitando compartirlas con otras personas y asegurando que se utilicen únicamente en entornos autorizados.
8. Es fundamental cerrar su sesión o bloquear el equipo al ausentarse, incluso por breves períodos, para prevenir accesos no autorizados.
9. Evitar instalar, modificar o desinstalar programas sin la aprobación del área correspondiente, con el fin de prevenir la introducción de amenazas al entorno institucional.
10. Manejar la información conforme a su nivel de sensibilidad (pública, interna, confidencial o restringida), siguiendo las medidas de protección correspondientes.
11. No compartir datos institucionales en redes sociales, medios digitales, conversaciones informales u otros canales, a menos que esté autorizado para hacerlo.
12. Contribuir activamente con sugerencias, buenas prácticas o lecciones aprendidas que ayuden a fortalecer el sistema de seguridad de la información.
13. Cambiar y/o actualizar las credenciales de acuerdo al nivel de usuarios que dispone, siendo para usuarios finales (con acceso a información sensible) el cambio de credenciales cada 90 días, para usuarios con acceso a sistemas críticos o con privilegios elevados (administradores, soporte, TI, OSI) el cambio de credenciales cada 60 días.
14. Retire toda la información y/o documentos de su escritorio físico, que incluyan datos de clientes, información institucional u otra que sea relevante, particularmente en lo que respecta a las transacciones financieras que se hayan llevado a cabo, recalcando especialmente cuando dicha información no esté en eso y/o el funcionario haya dejado su espacio de trabajo.

4.8. Propietarios y custodios de la información

1. Definir y mantener actualizada la clasificación de la información (pública, interna, confidencial o restringida) con base en su sensibilidad, criticidad y marco legal vigente.
2. Determinar quiénes pueden acceder a la información bajo su responsabilidad y en qué condiciones, asegurando que solo personal autorizado tenga acceso, conforme al principio mínimo de privilegio.
3. Colaborar estrechamente con los custodios de información (como TI o bases de datos) para asegurar que los controles implementados sean eficaces y acordes a las necesidades de la institución.

4. Verificar de forma regular los perfiles y permisos de accesos, solicitando revocación o modificación cuando sea necesario.
5. Coordinar con el Oficial de Seguridad de la Información para implementar las medidas de seguridad necesarias para salvaguardar la información bajo los principios de confidencialidad, integridad y disponibilidad de la información.
6. Implementar y apoyar en la ejecución de planes de continuidad y recuperación en caso de interrupciones, asegurando la restauración de la información en los tiempos establecidos.
7. Realizar respaldos seguros y confiables, verificar su integridad y consérvalos según la frecuencia y plazos definidos en la política institucional.
8. Registrar eventos significativos, accesos y cambios sobre la información o sus sistemas y alertar sobre actividades sospechosas o no autorizadas.
9. Emplear técnicas aprobadas para la eliminación definitiva de datos y soportes que ya no se utilicen, garantizando que no puedan ser recuperados por terceros.
10. Notificar inmediatamente al Oficial de Seguridad de la Información y al propietario de la información sobre fallos, vulnerabilidades o incidentes relacionados con la custodia de datos.

4.9. Usuarios externos-terceros

1. Aceptar y actuar conforme a las políticas internas de seguridad de la información de la institución, así como cualquier cláusula contractual relacionada con la protección de datos personales.
2. Garantizar la confidencialidad, integridad y disponibilidad de la información a la que acceden o que procesan como parte de su relación contractual o colaborativa con la institución.
3. Emplear únicamente los accesos, sistemas y herramientas que hayan sido específicamente asignados para sus funciones, evitando cualquier intento de acceso no autorizado.
4. No divulgar ni compartir información institucional con terceros no autorizados, ni utilizarla para fines distintos a los expresamente establecidos en el acuerdo o contrato.
5. Informar de inmediato al punto de contacto institucional si detectan anomalías, errores, accesos indebidos o situaciones que puedan poner en riesgo la seguridad de la información.
6. No delegar a terceros las tareas o accesos relacionados con la información institucional sin consentimiento formal por parte de la entidad contratante.
7. Destruir, devolver o cifrar toda información obtenida en el marco de la relación con la institución una vez finalizado el contrato o servicio, conforme a los procedimientos establecidos.
8. Asistir a sesiones de inducción, firmar compromisos de confidencialidad y seguir las indicaciones específicas de seguridad requeridas por la institución, especialmente en entornos sensibles.
9. Aceptar que la institución pueda revisar, auditar o verificar el cumplimiento de las obligaciones contractuales en materia de seguridad de la información, dentro de los límites establecidos.
10. Asegurarse de que el tratamiento de cualquier dato personal se realice de forma legal, ética y conforme a la normativa vigente, como la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador.

5. POLÍTICAS ESPECÍFICAS DE LA SEGURIDAD DE LA INFORMACIÓN.

5.1. Sensibilización en el campo de la Seguridad de la Información

El Oficial de Seguridad de la Información deberá participar conjuntamente con la Dirección de Talento Humano, Coordinación General de Planificación y Gestión Estratégica y la Dirección de Comunicación en la creación de un plan de capacitación anual para las partes interesadas (clientes, servidores públicos y otros).

1. El plan de capacitación estará dirigido a todo el personal en general, cargos con funciones críticas, alta dirección, nuevos ingresos y terceros.
2. El plan de capacitación debe incluir temas tales como:
    a) Buenas prácticas de uso de activos
    b) Fundamentos de seguridad de la Información

c) La importancia de la seguridad de la información en la función pública.
d) Clasificación y manejo de la información y el tratamiento adecuado de cada tipo.
e) Gestión de incidentes, cómo reportar y actuar ante un incidente.
f) Riesgos y amenazas significativas en el ámbito de la seguridad de la información, la ciberseguridad y la protección de datos personales.

5.2. Gestión de Activos

5.2.1 Control de Activos

1. Se entiende por activo de información a cualquier dato o elemento vinculado a su gestión, incluyendo bases de datos, documentación de sistemas, manuales de usuario, material de capacitación, protocolos operativos o de asistencia, plan de recuperación empresarial (BRP), plan de recuperación ante desastres (DRP) e información almacenada.
2. Se clasificarán como activos de información los siguientes elementos:
   a) Información: incluye todos los datos y documentos generados, recibidos o gestionados por la institución, sin importar su formato o medio de almacenamiento. Esta categoría comprende tanto información digital como física, incluyendo contratos, bases de datos, actas, resoluciones, reportes técnicos y administrativos y comunicaciones institucionales.
   b) Sistemas de información: son las aplicaciones, plataformas y herramientas informáticas utilizadas para procesar, almacenar o transmitir información institucional. Entre ellos se incluyen el sistema de gestión de compras públicas, los sistemas de gestión documental, plataformas de trámite y portales web.
   c) Equipos de cómputo y dispositivos tecnológicos: comprenden todos los dispositivos físicos que permiten el procesamiento y uso de la información, tales como computadoras de escritorio, laptops, teléfonos IP, servidores, entre otros.
   d) Soportes de información: incluyen medios físicos y digitales que contienen información institucional, como discos duros, memorias USB, CDs, DVDs, cintas de respaldo, carpetas físicas y documentos impresos.
   e) Infraestructura de Redes y Comunicaciones: corresponde a los elementos tecnológicos que permiten la transmisión y comunicación de datos dentro y fuera de la institución. Incluye redes cableadas e inalámbricas, enrutadores, firewalls, switches, VPNs y demás dispositivos o servicios que aseguran la conectividad institucional.
   f) Servicios Externos y Proveedores de Tecnología: incluyen servicios contratados como almacenamiento en la nube, plataformas de software como servicio (SaaS), servicios de hosting, correo electrónico institucional y proveedores tecnológicos.
   g) Entornos Físicos y Espacios de Trabajo: comprenden las oficinas, centro de datos, salas técnicas, archivos físicos y cualquier espacio donde se resguarden o procesen activos de información.
3. Se mantendrá un inventario actualizado de todos los activos de información, incluyendo hardware y software, medios digitales, documentos y datos. Este inventario debe identificar claramente a cada activo, su propietario, su clasificación y su ubicación, el inventario será revisado periódicamente para garantizar si vigencia, exactitud y completitud.
4. Cada activo deberá tener un responsable designado, quién será el encargado de garantizar su protección, uso adecuado y cumplimiento de las políticas de seguridad. Las responsabilidades del custodio incluyen su mantenimiento, control de acceso, respaldo (si aplica) y reporte de incidentes relacionados.
5. Los activos serán clasificados en función de su valor, criticidad y sensibilidad de la información que contienen o bien en la función que cumplen, asegurando que los activos críticos y sensibles reciban medidas de seguridad proporcionales a su importancia.

6. Se establecerán directrices claras sobre el uso adecuado de los activos institucionales, el personal deberá emplearlos únicamente para fines autorizados que le permitan el cumplimiento de sus funciones. El uso indebido o no autorizado de los activos será considerado una falta y estará sujeto a acciones disciplinarias conforme al reglamento interno.
7. Todo traslado, cesión o disposición final de activos deberá realizarse bajo procedimientos controlados que garanticen la protección de la información contenida o relacionada. Si el activo va a ser eliminado o reutilizado, se deberán aplicar técnicas seguras de borrado o destrucción, especialmente en activos que contenga información clasificada o confidencial.
8. Los activos deberán contar con controles físicos y/o lógicos que impidan accesos no autorizados, manipulación indebida, pérdidas o daños, de acuerdo con su criticidad.
9. Todo cambio significativo en los activos (por ejemplo, reemplazo, actualización, reasignación) deberá ser registrado y aprobado conforme a los procedimientos del SGSI, garantizado la trazabilidad y continuidad de las operaciones
10. El cumplimiento de estas políticas será evaluado mediante auditorías internas periódicas. Cualquier hallazgo deberá ser corregido mediante acciones de mejora que fortalezcan la gestión de los activos.

5.2.2 Inventarios de Activos

1. Toda unidad organizacional que posea, administre o utilice activos de información deberá mantener un inventario formal de los mismos, en el marco del Sistema de Gestión de Seguridad de la Información (SGSI). La actualización del inventario será una condición obligatoria para la gestión efectiva de riesgos y la protección de la información institucional.
2. El inventario debe contemplar todos los activos que intervienen en el tratamiento, almacenamiento, transmisión o respaldo de información institucional. Esto incluye, pero no se limita a: Equipos físicos (servidores, computadores de escritorios, laptops), Archivos de Software (sistemas operativos, aplicaciones, licencias), Información en soporte físico o digital (bases de datos, archivos, documentos), Servicios (infraestructura en la nube, servicios externos, redes) y Medios de Almacenamiento (USB, discos externos, CDs).
3. Cada activo de información registrado en el inventario debe contar con la siguiente información como mínimo: nombre o identificación única, tipo de activo, ubicación física o lógica, responsable designado, clasificación de la información asociada, estado (activo, en desuso, dado de baja), fecha de registro y fecha de última actualización.
4. El inventario de activos debe ser revisado y validado al menos una vez al año o cada vez que ocurra una modificación relevante (adquisición, traslado, baja o reasignación de activos), garantizando que la información del inventario sea precisa, completa y coherente con la realidad operativa.
5. Cada activo deberá contar con un nivel de criticidad definido, que permita aplicar controles de protección adecuados a su valor para la institución.
6. El inventario contiene información sensible sobre la infraestructura y recursos críticos de la institución. Por lo tanto, su acceso estará restringido únicamente al personal autorizado y su uso será exclusivo para fines de gestión de la seguridad de la información.

5.3. Administración de la Seguridad relacionada con los servidores públicos y partes interesadas

1. Todos los servidores, sin distinción de jerarquía o función, tienen la responsabilidad de proteger la información que manejan en el ejercicio de sus labores. Esta protección abarca tanto los datos internos de la institución como aquellos compartidos por ciudadanos, proveedores u otras identidades relacionadas. La seguridad de la información no es una tarea exclusiva del área técnica, sino una responsabilidad compartida que debe ser asumida con seriedad y ética profesional.

2. Los accesos a sistemas, documentos y aplicaciones estarán limitadas al mínimo necesario para cumplir con las funciones asignadas. Ningún servidor deberá acceder, modificar o divulgar información a la que no tenga autorización expresa. El uso de la información debe responder exclusivamente a fines institucionales, evitando cualquier aprovechamiento personal, político o comercial.
3. Toda información clasificada como confidencial o sensible debe ser protegida con medidas adecuadas, tanto técnicas como organizativas. Esta confidencialidad se mantiene incluso después de que el servidor público haya finalizado su relación laboral con la institución.
4. Se promoverá de forma constante la capacitación de los servidores sobre buenas prácticas de seguridad, normativas vigentes y los riesgos más comunes que puedan afectar la confidencialidad, integridad y disponibilidad de la información institucional.
5. Todos los servidores y partes interesadas deben reportar de manera inmediata cualquier sospecha, incidente o anomalía que pueda comprometer la seguridad de la información. La detección temprana y el reporte responsable son clave para mitigar impactos y evitar daños mayores. No se tolerará el encubrimiento de incidentes por temor a represalias o por desconocimiento de los canales de comunicación establecidos.
6. Cuando se establezcan relaciones con proveedores, contratistas o aliados estratégicos, la institución deberá garantizar que estos cumplan con los estándares de seguridad que maneja la institución. Toda transferencia de información estará sujeta a acuerdos de confidencialidad y cláusulas de seguridad que prevengan accesos no autorizados o usos indebidos.
7. La implementación de estas políticas será evaluada periódicamente, con el fin de detectar posibles brechas y fortalecer los controles existentes. Se fomentará una retroalimentación abierta entre los servidores y las áreas responsables para mejorar los procesos y adaptarse a nuevos desafíos.
8. De la información categorizada como confidencial o sensible debe permitirse el acceso al público, cumpliendo con el correcto flujo, el cual es tener la debida autorización y justificación para conceder el acceso, permitiendo así el derecho al acceso de la información de la normativa vigente.

5.4. Administración de la Seguridad relacionada con clientes y ciudadanos en general

1. SERCOP cuenta con un portal web que proporciona información sobre todos los servicios y procesos disponibles para los ciudadanos. SERCOP será responsable del manejo y uso de los datos personales obtenidos a través de este portal institucional, garantizando que dichos datos sean tratados con el más alto nivel de cuidado, de acuerdo con las normativas nacionales vigentes.
2. Todos los servicios digitales que la institución brinda están protegidos por mecanismos de seguridad que garanticen la autenticidad del portal web, la integridad de la información y la confidencialidad de los datos ingresado por el usuario. Se dispone de controles para prevenir fraudes, suplantación de identidad y cualquier tipo de vulneración que pueda afectar a los ciudadanos.
3. Bajo ningún concepto se permitirá el uso de datos con fines distintos a los autorizados, ni se compartirá con terceros sin una base legal o el consentimiento correspondiente.
4. Cada ciudadano tiene derecho a conocer qué información suya posee la institución, a solicitar su corrección si está equivocada y en los casos que la ley lo permita, solicitar su eliminación. Estos derechos serán respetados y gestionados a través de canales claros, sin barreras innecesarias ni demoras injustificadas.
5. Nuestras decisiones tecnológicas, políticas de seguridad y procesos administrativos estarán siempre orientados a proteger los datos de quienes confían en nosotros. La seguridad de la información no es solo un deber institucional, es un compromiso ético con la sociedad.
6. En caso que se produzca una vulneración que afecte a la información de los ciudadanos, la institución actuara con responsabilidad y prontitud. Se informará a los afectados en el menor tiempo posibles, se activarán los debidos protocolos de respuesta ante incidentes, permitiendo aplicar medidas correctivas para la continuidad de las operaciones. La comunicación será transparente, sin ocultar ni minimizar el impacto.

5.5. Administración en Áreas de Trabajo

5.5.1 Seguridad Física y del Entrono

1. La institución reconoce que un aspecto fundamental de la seguridad de la información está presente en el resguardo físico de sus instalaciones. Por esta razón, implementa y actualizará las medidas que eviten accesos no autorizados, daños intencionales o accidentes que puedan comprometer los recursos tecnológicos, documentales y humanos.
2. El acceso a las áreas de trabajo está regulado mediante mecanismos de control físico adecuados a su nivel de criticidad.
3. El Oficial de Seguridad de la Información en colaboración con la Coordinación Técnica de Innovación Tecnológica y los Propietarios de Información, según sea necesario, implementarán las medidas de seguridad física y ambiental para proteger los activos críticos, basándose en un análisis de riesgos y supervisará su ejecución. Además, se asegurará de que cumplan las normativas relacionadas con la seguridad física y ambiental.
4. Todo equipo que procese, almacene o transmita información institucional será protegido contra manipulación indebida, robo o deterioro. Los equipos de cómputo portátiles y de escritorio deberán siempre tener las sesiones bloqueadas cuando no estén en uso y almacenados de manera segura cuando no se use un periodo largo de tiempo. Antes de desechar cualquier equipo, se deberá asegurar la eliminación segura de la información que contenga.
5. Toda persona externa a la institución que requiera ingresar a las instalaciones deberá registrarse, estar acompañada por personal responsable y acceder únicamente a las áreas necesarias para el cumplimiento de su tarea. Se establecerán políticas claras para el ingreso de proveedores, técnicos externos o auditores, asegurando que su presencia no comprometa la seguridad física ni de la información.
6. Se fomentará entre todos los colaboradores una cultura de seguridad física, que incluya la protección de su entorno de trabajo, el uso correcto de credenciales de accesos, el reporte inmediato de anomalías y el respeto a las normativas establecidas. La seguridad no solo depende de los sistemas, sino también de las acciones cotidianas de cada persona dentro de la organización.

5.5.2 Seguridad en Oficinas e Instalaciones

1. Las oficinas e instalaciones de la institución deben ser espacios seguros, donde se garantice tanto la integridad del personal como la protección de los recursos que se manejan. Se establecerán controles y prácticas que prevengan riesgos físicos, accesos no autorizados o incidentes que puedan afectar la continuidad operativa o comprometer la información institucional.
2. Los servidores en todo momento deben llevar su credencial, permitiendo identificarlo de manera correcta.
3. Se fomentará entre los servidores una cultura de orden y protección de los espacios de trabajo. Documentos, dispositivos y equipos deben mantenerse bajo resguardo, especialmente al finalizar la jornada laborar. Las estaciones de trabajo no deben quedar expuestas con información sensible visible y todo material confidencial en formato físico deberá guardarse en archivadores seguros o cerrados con llaves.
4. Las salas de reuniones, áreas comunes y otros espacios compartidos estarán sujetos a reglas de uso que garanticen la confidencialidad de las discusiones y el resguardo de la información expuesta. Todo documento, presentación o dispositivo utilizado en esos espacios deberá ser retirado o asegurado al finalizar su uso.
5. Se asegurará que todas las instalaciones cuenten con señalización visible para rutas de evacuación, ubicación de extintores, puntos de reunión y otras medidas de seguridad. Además, se mantendrán accesibles los equipos de respuesta ante emergencias, como botiquines o alarmas y se capacitará periódicamente al personal para su uso adecuado.

5.5.3 Seguridad en los Equipos Institucionales

1. Los equipos tecnológicos utilizados en la institución, sean estos equipos de cómputo de escritorio o portátiles, servidores, periféricos, son activos esenciales para la operación diaria y el manejo seguro de la información. Su uso, resguardo y mantenimiento deben regirse por principios de responsabilidad, confidencialidad y continuidad operativa.
2. Todo equipo entregado al personal institucional será asignado mediante un registro formal, en el que se detallarán las condiciones de uso, los compromisos de cuidado y las restricciones aplicables. Cada servidor será responsable del buen uso del equipo bajo su cargo, evitando prácticas que puedan afectar su funcionamiento o poner en riesgo la información contenida en él.
3. Los equipos deben ser configurados por personal autorizado cumpliendo con guías de hardening de sistemas operativos por ejemplo Windows y Linux por la Dirección de Infraestructura y Operación. Esto incluye la instalación de software permitido, la activación de mecanismos de protección (antivirus, EDR, XDR, reglas de firewalls, cifrado, etc.) y la aplicación de políticas de actualización del sistema operativo. No se permitirá la modificación de configuraciones ni la instalación de programas que no se encuentren debidamente analizados y registrados en el inventario de software permitido.
4. Los usuarios deberán seguir las recomendaciones institucionales para respaldar de manera periódica la información crítica contenida en los equipos. Los respaldos deberán almacenarse en medios confiables y bajo control institucional. Ante cualquier pérdida de datos o fallas técnicas, se deberá reportar de inmediato al área correspondiente para activar los mecanismos de recuperación.
5. Antes de desechar, reasignar o devolver un equipo, se deberá garantizar la eliminación segura de toda la información almacenada. Esta tarea será gestionada exclusivamente por personal autorizado, utilizando métodos que impidan la recuperación posterior de los datos. Ningún equipo podrá ser entregado a un tercero sin pasar por este proceso.
6. Los equipos deben conectarse únicamente a redes y servicio autorizados por la institución. Está prohibido vincular equipos personales no registrados a las redes internas sin una evaluación de riesgos y aprobación previa. El uso de dispositivos externos de almacenamiento (como USB, discos duros) no pueden ser utilizados en los equipos de cómputo de la institución para prevenir la introducción de malware o fugas de información.

5.6. Gestión de Infraestructura y Operaciones

5.6.1 Internet y Correo Electrónico

1. El acceso a correos electrónicos personales y redes sociales está restringido en todos los dispositivos de la institución, excepto para aquellos servidores cuya labor requiera interactuar con dichos medios de comunicación. En estos casos, considerados como permisos especiales de navegación, el funcionario deberá presentar la solicitud correspondiente al área pertinente, para la autorización del Director del área y posteriormente el Oficial de Seguridad de la Información dará su aprobación, generando un ticket para que soporte otorgue los permisos necesarios.
2. Toda información sensible o confidencial que se transmita por correo electrónico deberá contar con mecanismos de protección adecuados, como cifrado, contraseñas o cualquier otro tipo de medio de verificación. No se debe compartir información personal, contraseñas, credenciales o archivos críticos sin asegurarse previamente de la identidad y autorización del destinatario.
3. Dado que el correo electrónico es un canal común de amenazas (como phishing, malware o ingeniería social), los usuarios deben evitar abrir mensajes sospechosos, enlaces desconocidos o archivos adjuntos no verificados. En caso de recibir un correo inusual o potencialmente malicioso deberá reportarse al Oficial de Seguridad de la Información.

4. La dirección de Infraestructura y Operaciones será la encargada de administrar las plataformas de correo electrónico y servicios de internet. Esto incluye la gestión de cuentas, monitoreo del uso, aplicación de filtros de seguridad, almacenamiento de respaldos y eliminación segura de cuentas inactivas. Toda configuración técnica será documentada y revisada de forma periódica.
5. La institución fomentará entre sus colaboradores la adopción de buenas prácticas en el uso de internet y correo electrónico, brindando capacitaciones, recomendaciones actualizadas y alertas ante nuevas amenazas. El personal deberá actuar con sentido común y mantenerse alerta frente a conductas sospechosas o riesgos digitales.
6. Todos los usuarios tendrán, por defecto, restricciones en su acceso a internet. Si un usuario desea obtener privilegios adicionales, deberá presentar una solicitud a través de la intranet en la mesa de soporte. Esta solicitud requerirá la aprobación de su Director de Área, quien evaluará la justificación y asumirá la corresponsabilidad de la excepción solicitada. Posteriormente, el Oficial de Seguridad de la Información dará su visto bueno y se generará un ticket para que la mesa de soporte lo atienda.

5.6.2 Respaldo de Datos

1. La información gestionada por la institución constituye uno de sus activos más preciados. Su perdida, alteración o indisponibilidad podría generar consecuencias graves en la operación, el cumplimiento normativo y la confianza ciudadana. Por esta razón se establece esta política para asegurar la existencia de copias de seguridad que sean confiables, actualizadas y accesibles ante cualquier eventualidad. Estas deberán ejecutadas por la Dirección de Seguridad Informática.
2. Las copias de seguridad deberán realizarse con una periodicidad definida según la criticidad de la información y los tiempos máximos tolerables de recuperación. En términos generales:
    a) Información crítica: respaldo diario.
    b) Información Operativa o de Soporte: respaldo semanal.
    c) Registros Históricos o Poco Cambiantes: respaldo mensual.

    La programación de los respaldos debe permitir su ejecución automática y sin interrupciones a los procesos activos.
3. Toda copia de seguridad debe almacenarse en medios seguros, con acceso controlado y protegidos contra pérdida, daño o acceso no autorizado. Se recomienda aplicar el principio 3-2-1 que consiste en mantener tres copias de seguridad de los datos, un respaldo local en medios distintos (discos duros externos, cintas magnéticas, etc.) y otro en entorno fuera del sitio (offside o en la nube) siempre bajo las mismas condiciones de seguridad.
4. Las copias de seguridad deben estar protegidas mediante cifrado, contraseñas y otros controles que impidan su alteración o uso indebido. Solo el personal debidamente autorizado podrá acceder, restaurar o modificar las copias de respaldo. Se debe evitar que las copias contengan errores, información obsoleta o archivos dañados.
5. No es suficiente con hacer copias de seguridad, también es crucial asegurarse de que se puedan restaurar adecuadamente cuando sea necesario. Por esta razón, se llevarán a cabo pruebas regulares de recuperación, tanto parciales como completas, para confirmar su operatividad. Estas pruebas deben ser registradas y ser parte del plan de continuidad institucional.
6. Cada copia de seguridad tendrá un período de retención previamente definido, según la normativa vigente y las necesidades operativas. Una vez cumplido este período, los respaldos serán eliminados de forma segura, garantizando que no quede rastro recuperable de la información eliminada.

5.6.3 Defensa contra Software Malicioso (Malware)

1. La presencia de software malicioso como virus, troyanos, spyware, ransomware y otros tipos de código dañino constituye una amenaza constante para la integridad, confidencialidad y disponibilidad de la información institucional. Es por ello que se deben establecer las medidas que deberán ser adoptadas para prevenir, detectar, responder y mitigar los efectos del malware en los sistemas, equipos y redes que la institución administra.
2. La mejor defensa contra el software malicioso es la prevención. Por esta razón todos los dispositivos institucionales deberán contar con herramientas actualizadas de protección (XDR), configurados para operar de forma continua y con actualizaciones automáticas activas. Ningún equipo podrá operar sin estas protecciones activas.
3. La institución mantendrá todos sus sistemas, aplicaciones y plataformas tecnológicas actualizadas con los parches de seguridad que liberen los proveedores. Las actualizaciones deberán aplicarse de manera planificada, con el objetivo de reducir al mínimo la interrupción de los servicios, pero sin postergar innecesariamente la corrección de vulnerabilidades conocidas.
4. Los servidores deben desempeñar un papel proactivo en la prevención del software malicioso. Se les capacitará regularmente para identificar señales de infección, evitar la apertura de correos electrónicos sospechosos, reconocer intentos de engaño (phishing) y reportar cualquier comportamiento extraño en sus equipos. La conciencia del usuario es un componente esencial del control preventivo.
5. Si se detecta un posible caso de infección por malware, el equipo afectado deberá ser aislado de la red para evitar su propagación y por ningún motivo debe ser apagado, de esta manera se puede identificar de manera oportuna Indicadores de Compromiso (IOCs). El área encargada aplicará los debidos procedimientos de análisis, contención, erradicación y recuperación, documentando todo el proceso. En caso de que el incidente haya comprometido datos sensibles, se activarán los protocolos de notificación y tratamiento establecidos en el SGSI.
6. El entorno de amenazas evoluciona constantemente. Por eso la institución estará evaluando de manera periódica la efectividad de protección contra software malicioso.

5.6.4 Gestión de Redes Administrativas

1. Las configuraciones de los dispositivos de red y seguridad, incluyendo ruteadores, switches, firewalls, IPS/IDS y otros dispositivos de seguridad informática, deben ser respaldadas y resguardadas adecuadamente por la Dirección de Seguridad Informática.
2. Los detalles sobre los diagramas de arquitectura y las configuraciones de red serán de conocimiento exclusivo de la Dirección de Infraestructura y Operaciones.
3. La Dirección de Infraestructura y Operaciones revisará y aprobará todo equipo antes de ser conectado a cualquier nodo de la red de datos institucional. Esta área tiene la responsabilidad de desconectar los dispositivos que no tengan la debida aprobación y reportar la conexión como incidente de seguridad. Además, se deberán deshabilitar los puntos de conexión de voz y datos que no estén en uso.
4. Cualquier red inalámbrica deberá requerir autenticación y asegurar la encriptación del tráfico.
5. El acceso remoto a la red de datos de SERCOP debe llevarse a cabo a través de una red privada virtual (VPN), la cual estará sujeta a controles y supervisión por parte de la Dirección de Seguridad Informática.
6. La autorización para el uso de la VPN deberá ser concedida por el Director de Seguridad Informática, Coordinador de Tecnologías de la Información y Telecomunicaciones, Oficial de Seguridad de la Información, mediante un formulario Acceso a VPN que el servidor tendrá que completar, el cual será aprobado y enviado su superior inmediato.

7. Es fundamental tener en cuenta que la red de datos institucional debe ser escalable, organizada y planificada, asegurando la disponibilidad de materiales, infraestructura de telecomunicaciones (como racks, routers, switchs, etc.) y la adecuada distribución del personal encargado de atender estas necesidades.

5.6.5 Gestión de Dispositivos Extraíbles de Almacenamiento

1. Se restringe el uso de dispositivos extraíbles en los equipos de cómputo tanto escritorio como laptops de la institución. Solo se podrán utilizar en casos justificados, cuando su uso esté autorizado por la Dirección de Infraestructura y Operaciones y siempre que se cumplan con los controles establecidos en esta política.
2. Cualquier dispositivo extraíble que vaya ser utilizado en el entorno institucional deberá estar previamente autorizado y registrado. Esta autorización debe estar fundamentada en una necesidad operativa clara y ser validada por el área correspondiente. Los dispositivos autorizados deberán identificarse con etiquetas o registros internos que permitan su trazabilidad.
3. Todos los dispositivos extraíbles deberán ser analizados con herramientas que permitan identificar, eliminar malware antes de su conexión a equipos institucionales. Este análisis debe realizarse de forma automática al insertare el dispositivo, o manualmente si se trata de sistemas críticos o sensibles. En caso de detectarse una amenaza, se procederá a su aislamiento y eliminación segura.
4. Cualquier información clasificada como sensible, confidencial o crítica que sea almacenada en un dispositivo de almacenamiento extraíble deberá estar cifrada o protegida mediante contraseñas. Además, está prohibido almacenar información institucional en dispositivos personales o no autorizados, así como transportar datos fuera de la institución sin justificación formal y medidas de resguardo.
5. El uso de dispositivos extraíbles de almacenamiento autorizados implica una responsabilidad directa por parte del usuario. Este deberá asegurarse de:
    a) No compartir el dispositivo con terceros sin autorización.
    b) Proteger físicamente el dispositivo contra pérdida o robo.
    c) Informar de inmediato en caso de extravío, daño o acceso no autorizado.
6. Los dispositivos que ya no se utilicen, o aquellos que deban ser desechados, deberán pasar por un proceso de eliminación segura de la información. Esto evitará que los datos almacenados puedan ser recuperados por personas no autorizadas. La eliminación deberá realizarse con herramientas especializadas o mediante la destrucción física del dispositivo, según el nivel de sensibilidad.

5.6.6 Gestión Segura de Baja y/o Destrucción de Información

1. La institución genera, almacena y gestiona grandes volúmenes de información, parte de la cual pierde vigencia, relevancia o utilidad operativa. La eliminación inadecuada de esta información puede derivar en filtraciones, accesos no autorizados o incluso en incumplimientos legales. Es por ello que se deben establecer los lineamientos para asegurar que la información y los medios que la contienen sean dados de baja de manera segura, controlada y conforme a los principios del SGSI y EGSI vigentes.
2. La Gestión Segura de Baja y/o Destrucción de Información deberá ser aplica a toda la información institucional independientemente del formato en el que se encuentre (digital, físico, audiovisual, etc.) y a todos los dispositivos o medios de almacenamiento que la contenga. Es de cumplimiento obligatorio para todo el personal, proveedores y partes interesadas que manipulen información de la institución.

3. Antes de eliminar información almacenada en sistemas, servidores, discos duros, memorias USB o cualquier otro medio digital, se deberán aplicar métodos que garanticen su no recuperación. Dependiendo de la sensibilidad de la información, se podrán emplear técnicas como:
    a) Borrado lógico con sobre escritura segura.
    b) Desvinculación segura de archivos y particiones.
    c) Cifrado irreversible seguido de un proceso de eliminación.
    d) Destrucción física del dispositivo cuando sea necesario.

   La simple eliminación del archivo (envío a la papelera de reciclaje o formateo simple) no se considerará una medida segura.
4. Para la información contenida en papel, discos ópticos, cintas magnéticas u otros formatos físicos, la destrucción deberá hacerse mediante mecanismos que garanticen que no pueda ser reconstruida ni interpretada posteriormente. Esto puede incluir:
    a) Trituración en partículas finas.
    b) Incineración controlada.
    c) Desintegración o compactación industrial.

   Los documentos con datos sensibles o clasificados no podrán ser desechados en papeleras comunes ni almacenados en lugares de fácil acceso antes de su destrucción.
5. Cada proceso de eliminación segura deberá ser registrada formalmente, incluyendo los siguientes elementos:
    a) Tipo de información eliminada.
    b) Medio o dispositivo que la contenía.
    c) Método de eliminación utilizada.
    d) Responsable de la ejecución.
    e) Fecha y observaciones relevantes.

   Estos registros permitirán auditorías posteriores y respaldarán la rendición de cuentas sobre el tratamiento adecuado de la información.
6. Cualquier dispositivo o equipo que se vaya a retirar del inventario institucional deberá pasar primero por un proceso de eliminación segura de la información que haya contenido. Esta tarea será responsabilidad exclusiva del personal autorizado del área técnica y quedará registrada en un acta de baja o formato similar.
7. La eliminación de información deberá realizarse conforme a la normativa vigente sobre protección de datos personales, archivos institucionales, transparencia y cualquier otro marco aplicable. En particular, deberá respetarse el tiempo mínimo de conservación exigido por ley o por normativas internas antes de proceder a su eliminación.

5.6.7 Control de Cambios

1. La Coordinación Técnica de Innovación Tecnológica será responsable de la segmentación de los recursos destinados al desarrollo, pruebas y producción, con el fin de evitar que la institución enfrente problemas operativos y cambios inesperados o no deseados en sus sistemas de información. Para ello se implementarán al menos los siguientes controles:
    a) Las actividades de desarrollo y prueba deberán ser ejecutados en entornos distintos.
    b) Estarán restringidos los accesos a compiladores, editores y otras herramientas del sistema en el entorno de producción, salvo que sean estrictamente imprescindibles para su operatividad.
    c) Se aplicarán sistemas de control de accesos junto con el sistema de múltiple factor de autenticación para cada uno de los entornos, así como perfiles de accesos específicos para los sistemas.
    d) El personal responsable de desarrollo no tendrá acceso al entorno de producción y en caso de que sea imprescindible, se establecerá un acceso especial el cual contará con la autorización, documentación y registro de dicho acceso.

2. Documentar todos los cambios relacionados con activos de información, componentes tecnológicos, configuraciones, procedimientos técnicos y servicios que puedan impactar la confidencialidad, integridad o disponibilidad de la información manejada por la institución, es de carácter obligatorio para el personal técnica, proveedores y cualquier área que impulse cambios sobre los sistemas institucionales.
3. Los cambios se clasificarán de acuerdo a su naturaleza de impacto:
    a) Cambios estándar: Modificaciones de bajo riesgo, recurrentes y previamente aprobadas (por ejemplo, actualizaciones menores).
    b) Cambios normales: Cambios planificados que requieren evaluación y autorización antes de su ejecución.
    c) Cambios urgentes: Cambios que deben realizarse de inmediato por motivos críticos (fallas, incidentes, vulnerabilidades graves). Se documentan a posteriori, pero con los mismos. criterios de trazabilidad.
4. Todo cambio que se realice en el entorno tecnológico de la institución debe estar debidamente planificado y analizado antes de su ejecución, considerando no solo los aspectos técnicos, sino también los posibles riesgos operativos y de seguridad que pudieran implicar. Cada modificación debe pasar por un proceso de evaluación, ser aprobada formalmente por los responsables designados y quedar documentada en un registro.
5. Todos los cambios deberán quedar documentados en un Registro de Cambios que contendrá como mínimo los siguientes puntos:
    a) Descripción del cambio.
    b) Justificación.
    c) Fecha de ejecución.
    d) Responsable(s).
    e) Aprobación.
    f) Resultados de las pruebas.
    g) Observaciones post implementación.

5.6.8 Teletrabajo

Con el fin de adaptarse a modelos laborales flexibles y garantizar la continuidad operativa de la institución se debe establecer por parte de la Dirección de Talento Humano en conjunto con el Oficial de Seguridad de la Información las condiciones necesarias para el uso seguro de la modalidad de teletrabajo. De esta manera se busca asegurar que incluso fuera de las instalaciones físicas de la institución, se mantenga la protección adecuada de la información institucional y se prevengan riesgos asociados al uso remoto de sistemas y recursos.

A continuación, se presentan ciertas directrices que deben tenerse en cuenta para fortalecer las medidas de seguridad en el teletrabajo:

1. Condiciones generales para el teletrabajo
    a) El teletrabajo deberá estar previamente autorizado por la institución y sustentado por una necesidad operativa.
    b) El personal deberá firmar un compromiso de confidencialidad y uso responsable de los recursos tecnológicos.
    c) Se establecerán controles para asegurar que el acceso remoto no comprometa la seguridad de la información, los sistemas ni los servicios críticos.
2. Requisitos de Seguridad Tecnológica
    a) El equipo utilizado debe contar con medidas de protección como EDR, XDR, antivirus actualizado, cifrado de disco y bloqueo de pantalla automático.

b) El acceso a los sistemas institucionales debe realizarse mediante canales seguros, como redes privadas virtuales (VPN), conexiones cifradas y el uso de autenticación multifactor.
c) Se prohíben el uso de redes públicas o no seguras para acceder a sistemas sensibles o manejar información clasificada.
d) El equipo no deberá ser compartido con personas no autorizadas ni usarse para actividades personales mientras esté conectado a los sistemas de la institución.

3. Protección de la información
   a) Se debe evitar almacenar información institucional de forma local en los dispositivos personales o externos, salvo que sea estrictamente necesario y autorizando.
   b) Toda la información generada o manejada durante el teletrabajo se considera propiedad institucional y está sujeta a las políticas de seguridad de la información.
   c) Si se requiere transportar información, esta deberá estar cifrada mediante mecanismos de acceso seguro.
4. Navegación Web y uso seguro de internet
   a) Los usuarios deben abstenerse de ingresar a sitios web no relacionados con sus funciones laborales, descargar archivos desde fuentes no confiables.
   b) Es recomendable eliminar periódicamente las cookies y los archivos temporales de todos los navegadores web que utilice.
   c) El personal deberá mantener una actitud vigilante ante posibles fraudes en línea, enlaces sospechosos o páginas que intenten recolectar información sensible sin autorización.

5.7. Administración de Accesos

5.7.1 Acceso a Servicios de Tecnología Informática

1. El acceso a los servicios informáticos será otorgado de acuerdo al principio de mínimo privilegio y conforme al rol y funciones asignadas al usuario dentro de la institución.
2. Todo acceso a servicios informáticos deberá estar protegido por mecanismos de autenticación seguros (por ejemplo: contraseñas robustas, autenticación multifactor, certificados digitales, entre otros, según la criticidad del sistema).
3. Se debe tener una gestión centralizada de cuentas de usuario, incluyendo la creación, modificación, suspensión y eliminación de accesos, así como el registro de sesiones activas y sus tiempos de inactividad.
4. Los accesos remotos a servicios informáticos deben realizarse únicamente mediante canales seguros (VPN, túneles cifrados u otros mecanismos aprobados) y solo estarán permitidos previa autorización formal.
5. Los accesos otorgados serán revisados de manera periódica para asegurar que estén actualizados y sean coherentes con las funciones del usuario. Cualquier acceso innecesario o indebido será revocado de inmediato.
6. Todos los accesos a servicios informáticos críticos deberán estar debidamente registrados mediante mecanismos de auditoría, que permitan identificar al usuario, el recurso accedido, la fecha y hora del acceso.
7. En caso de requerirse accesos temporales (por ejemplo, para soporte técnico o auditorías), estos deberán estar limitados en tiempo y alcance y documentarse adecuadamente.
8. Los accesos a servicios informáticos deberán ser revocados de inmediato cuando un usuario cambie de función, finalice su relación contractual o se detecte un uso indebido.

9. Cada usuario debe tener, por defecto, acceso restringido a los distintos módulos informáticos, así como a los repositorios de información que no estén relacionados con su gestión, de acuerdo con los procesos y competencias definidas. Para obtener accesos adicionales, es necesario que el Director del Área lo solicite de manera justificada a través de la mesa de soporte, informando al Oficial de Seguridad de la Información.
10. Disponer de estos puntos dentro del proceso de administración de accesos a los activos de información:
    a) Solicitud de accesos
    b) Autorización de accesos
    c) Ejecución de accesos
11. Es fundamental clasificar al menos dos categorías de usuarios y/o cuentas en relación con sus activos de información. Por un lado, se encuentran los usuarios finales, que pueden ser genéricos, temporales u operativos y que acceden a los sistemas de información de manera cotidiana, estando sujetos a políticas de contraseñas, caducidad y monitoreo. Por otro lado, están los usuarios privilegiados, como los transaccionales o root, que poseen permisos elevados para la configuración, mantenimiento y administración de sistemas y su uso debe ser restringido y controlado de manera rigurosa.
12. Controlar que todo usuario que ha dejado de prestar sus servicios en la institución debe entregar todos los dispositivos asignados a él (como tarjetas de accesos, computadores, entre otros) y ser desactivado de todos los accesos a servicios informáticos de la institución (tales como acceso a servidores, bases de datos, firewalls, routers, switchs, entre otros).
13. Para estaciones de trabajo (pc, laptops, terminales) el bloqueo automático de la sesión debe activarse tras un tiempo máximo de inactividad de 2 minutos, este bloqueo debe requerir autenticación del usuario para reactivar la sesión (por ejemplo, contraseña o mecanismo biométrico).
14. Los accesos remotos de administración (SSH,Telnet, consola web) a dispositivos de red (switches, routers, firewalls,etc) deben configurarse para cerrarse automáticamente tras un periodo máximo de inactividad de 2 minutos, además se debe implementar restricciones de IP origen, autenticación multifactor y en lo posible VPN para canal seguro.
15. Toda cuenta sea de estaciones de trabajo o para accesos remotos de administración debe bloquearse luego de tres intentos fallidos y para su desbloqueo deberá contactarse con el área correspondiente.
16. Las cuentas de usuario que permanezcan inactivas durante un periodo continuo de 90 días serán desactivadas automáticamente, a excepción de aquellas cuentas de servicio que cuenten con una justificación adecuada.
17. Las cuentas con privilegios deben ser supervisadas con mayor regularidad y desactivadas después de un periodo de inactividad de 30 a 60 días continuos, dependiendo de la criticidad del sistema.
18. Las cuentas destinadas a proveedores y/o genéricas, como las de control y operativas, deben ser solicitadas por el área correspondiente, incluyendo la documentación necesaria como instrumentos legales, memorandos u oficios y se debe indicar quién será el responsable de su custodia. Al concluir la actividad para la que se solicitaron, el usuario y/o cuenta será desactivado.

5.7.2 Gestión de Contraseñas y Nombres de Usuarios

1. Definir normas seguras y coherentes para la creación, asignación, utilización y resguardo de nombres de usuario y contraseñas en los sistemas de la institución, asegurando que únicamente individuos autorizados tengan acceso a la información y a los recursos tecnológicos de la institución.
2. Todos los servidores, proveedores, contratistas y terceros que accedan de manera directa o remota, a sistemas, plataformas, aplicaciones o dispositivos que contengan información de la institución, independientemente de su nivel de criticidad tienen la responsabilidad de cumplir con los lineamientos descritos.

3. Todos los servidores, proveedores, contratistas y terceros que tengan autorización para acceder a los sistemas de la institución recibirán un nombre de usuario exclusivo e intransferible, que estará vinculado a su identidad y a las funciones que desempeñan en la institución.
4. Las credenciales o datos sensibles no deben pegarse en pantallas, escritorios o monitores, ni mantenerse visibles en pizarras u hojas sueltas.
5. Está prohibido compartir cuentas o credenciales entre personas, salvo en situaciones excepcionales previamente justificadas y aprobadas.
6. Es fundamental que las contraseñas sean fuertes, evitando el uso de información personal obvia como fechas, nombres o números de identificación. Deben tener al menos 12 caracteres y combinar letras en mayúsculas y minúsculas, números y símbolos especiales.
7. Se recomienda el uso de frases de paso (passphrases) para mejorar la memorización sin sacrificar seguridad.
8. El sistema requerirá que las contraseñas se cambien de manera regular, al menos cada 90 días, o de acuerdo con el nivel de acceso del usuario.
9. Las contraseñas no deben ser reutilizadas, ni almacenadas en papel o en archivos no cifrados, se recomienda utilizar gestores de contraseñas para su almacenamiento y gestión. Así también se prohíbe el uso de la misma contraseña en sistemas personales e institucionales.
10. Los nombres de usuario se otorgarán con los permisos mínimos necesarios para realizar las tareas laborales, previniendo accesos no autorizados a sistemas o información sensible.
11. Cualquier ampliación de privilegios deberá estar sustentada y con aprobación explícita del Oficial de Seguridad de la Información y del área correspondiente.
12. Cada usuario tiene la responsabilidad directa de asegurar el uso adecuado, la protección y la confidencialidad de sus credenciales. Por lo tanto, es fundamental que cambie su contraseña tan pronto como sospeche que ha sido comprometida. No debe permitir que terceros utilicen su cuenta, ni siquiera de manera temporal y debe informar al Oficial de Seguridad de la Información sobre cualquier acceso no autorizado o intento sospechoso de acceso a su cuenta.

5.7.3 Gestión de Pantalla Limpia y Área de Trabajo

1. Establecer lineamientos claros para mantener el escritorio del sistema operativo libre de accesos directos innecesarios, archivos temporales o carpetas personales, de igual manera mantener despejado el escritorio del área de trabajo, con el fin de reducir riesgos de exposición, perdida o acceso no autorizado a información institucional.
2. El escritorio del computador institucional deberá mantenerse lo más despejado posible. No debe utilizarse como espacio de almacenamiento de trabajo permanente.
3. No se debe colocar accesos directos a sistemas, plataformas o aplicaciones que gestionen información clasificada, sensible o confidencial, especialmente si no cuentan con mecanismos de autenticación robusta.
4. Archivos que contengan datos institucionales, informes internos, información de usuarios o configuraciones técnicas deben mantenerse en ubicaciones seguras dentro de las unidades cifradas o carpetas protegidas, nunca en el escritorio.
5. Las áreas de trabajo deben mantenerse organizadas, sin documentos sensibles expuestos a la vista o al alcance de terceros. Se debe fomentar una cultura de seguridad basada en la responsabilidad individual sobre el entorno físico.
6. Al ausentarse de su puesto, aunque sea por poco tiempo, el usuario deberá bloquear la sesión del computador.
7. Documentos en papel que contengan información clasificada o restringida deben guardarse en cajones o archivadores bajo llave cuando no se estén utilizando.
8. Es recomendable restringir el acceso a las fotocopiadoras e impresoras fuera del horario laboral habitual para evitar su uso no autorizado.
9. El Oficial de Seguridad de la Información, en conjunto con la Coordinación General de Planificación y Gestión Estratégica, llevará a cabo revisiones periódicas de pantallas, escritorios y áreas de trabajo limpias, siguiendo las recomendaciones establecidas:

a) Se realizará una revisión por muestreo de los equipos de cómputo (Escritorio y Portátiles).
b) Esta inspección se ejecutará durante las auditorías internas que la organización planifique. La cantidad de accesos directos deberán cumplir con lo estipulado en la documentación de hardening del sistema operativo.
c) Bajo ninguna circunstancia se deben mostrar íconos de carpetas en el escritorio, así como tampoco se deben dejar a la vista los nombres de documentos que sean reservados o confidenciales.

5.7.4 Gestión de Accesos de Usuarios

5.7.4.1 Asignación de Roles

1. Establecer criterios y lineamientos claros para la asignación de roles de usuario, sus niveles de privilegio y sus responsabilidades asociadas, con el objetivo de asegurar un control adecuado sobre el acceso a los sistemas, datos y servicios tecnológicos de la institución, reduciendo riesgos y asegurando el principio de mínimo privilegio.
2. El acceso se otorga con base en las funciones laborales o contractuales del usuario, no de manera indiscriminada ni por conveniencia.
3. Cada usuario contará únicamente con los permisos estrictamente necesarios para realizar sus tareas. No se asignarán accesos preventivos o excesivos.
4. Todo acceso será asignado a un usuario individual, con credenciales únicas e intransferibles. No se permiten cuentas compartidas, salvo casos excepcionales debidamente autorizados.
5. La Dirección de Seguridad de la información, en conjunto con el Oficial de Seguridad de la Información, será responsable de definir los roles estándar dentro de cada sistema o aplicación.
6. Cada rol debe estar documentado, con una descripción clara de las funciones, niveles de acceso, privilegios y restricciones.
7. Los accesos no serán asignados directamente a cuentas personales, sino a través de roles previamente definidos y aprobados.

5.7.4.2 Responsabilidades y privilegios de accesos (roles) otorgados a usuarios

1. Los derechos y privilegios de acceso se otorgarán en función de la necesidad de utilizar el activo de información y las demandas de los usuarios.
2. Cada rol de usuario institucional conlleva un conjunto específico de responsabilidades asociadas al uso de la información.
3. Los usuarios operativos serán responsables de manejar información dentro del marco de sus funciones diarias, sin capacidad de administración ni modificación de parámetros del sistema.
4. Los usuarios administrativos pueden gestionar configuraciones o realizar tareas técnicas, bajo supervisión y con registro de actividades.
5. Los supervisores o líderes de área serán responsables de validar las solicitudes de acceso de su equipo, revisar periódicamente los privilegios otorgados y comunicar cualquier cambio funcional relevante.
6. Los administradores de sistemas o datos tendrán la responsabilidad de configurar, mantener y auditar los accesos en los entornos técnicos bajo su control. Su accionar debe estar sujeto a monitoreo constante y doble control cuando sea posible.
7. El listado de roles, sus descripciones y privilegios asociados deberá revisarse al menos una vez al año o cuando existan cambios relevantes en procesos, sistemas o estructuras organizacionales.
8. Se deben realizar controles periódicos para verificar que los accesos asignados se mantengan alineados con los roles vigentes de los usuarios y que no existan acumulaciones indebida de privilegios.

5.7.4.3 Responsabilidades y privilegios de accesos (roles) especiales

1. Se considera acceso especial a cualquier permiso o privilegio que exceda los niveles de acceso estándar y que permita administrar usuarios, contraseñas o permisos, configurar o modificar parámetros críticos del sistema, acceder a información clasificada, confidencial o sensibles, manipular infraestructura tecnológica o servicios en producción, ejecutar comandos de alto riesgo o realizar mantenimiento sin supervisión directa.
2. El acceso especial sólo se otorga cuando exista una necesidad operativa o técnica real, justificada y documentada.
3. Siempre que sea posible, los accesos especiales deben tener un tiempo de vigencia definido y expirar automáticamente cuando ya no sean necesarios.
4. Se debe mantener un registro actualizado de todos los usuarios con privilegios especiales, detallando los sistemas involucrados, nivel de acceso, fecha de asignación y personal que autoriza.
5. Cada uso de estos privilegios debe ser registrado y los registros deben mantenerse disponibles para auditorías internas o externas.
6. Usar dichos privilegios única y exclusivamente para los fines autorizados.
7. Evitar ejecutar acciones no solicitadas o fuera del alcance de la tarea aprobada.
8. No delegar, compartir o transferir sus credenciales bajo ninguna circunstancia.
9. Documentar adecuadamente los cambios realizados y notificar cualquier resultado inesperado o fallo.
10. Mantener la confidencialidad absoluta sobre la información a la que tenga acceso, especialmente si es sensible o clasificada.
11. Se realizarán revisiones periódicas (al menos semestrales) para evaluar la vigencia y necesidad de mantener cada acceso especial activo.
12. Cuando sea posible, el uso de estos privilegios deberá estar protegido mediante mecanismos adicionales como doble factor de autenticación o el uso de herramientas de gestión de accesos privilegiados (PAM).

5.7.4.4 Creación de Usuarios

1. Toda solicitud de creación de una cuenta debe ser tramitada a través del canal oficial designado (por ejemplo, mesa de ayuda o formulario institucional.).
2. El responsable del área deberá justificar la necesidad del acceso e indicar claramente los privilegios requeridos, según el rol o funciones del usuario.
3. La Dirección de Seguridad Informática verificará la solicitud, asignará el perfil correspondiente y generará las credenciales iniciales de forma segura.
4. Al usuario se le informará sobre el uso correcto de sus credenciales y las políticas asociadas (contraseñas, privilegios, restricciones de uso, etc.).
5. Cada cuenta deberá asociarse a un identificar único que permita rastrear y auditar su uso dentro de los sistemas.

5.7.4.5 Des habilitación y Eliminación de Usuarios

1. Al finalizar la relación laboral o contractual, los accesos de los usuarios deberán ser revocados o des habilitados el mismo día de la desvinculación.
2. En casos de licencias prolongadas, vacaciones o ausencias injustificadas, la cuenta podrá ser suspendida temporalmente a solicitud del área responsable.
3. Las cuentas inactivas por más de 90 días serán revisadas y podrán ser des habilitadas automáticamente, previa verificación.

4. Los archivos, correos y recursos asociados a una cuenta des habilitada deberán ser gestionados conforme a las políticas de continuidad, respaldo y traspaso de información.

5.7.4.6 Gestión de Accesos por Parte de Terceros

1. Los puntos mencionados en esta sección se enfocarán en la protección de la información ante individuos o entidades externas, sin menoscabo de lo dispuesto por la legislación gubernamental establecida en la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP).
2. En situaciones donde se requiera proporcionar acceso a la información empresarial a terceros, será responsabilidad del Oficial de Seguridad de la Información aprobar dicha solicitud, teniendo en cuenta lo siguiente:
    a) El tipo de acceso solicitado, ya sea físico o lógico y el recurso específico al que se desea acceder.
    b) Las razones que justifican la solicitud.
    c) Las medidas de seguridad implementadas por la parte solicitante y el impacto que este acceso podría tener en la seguridad de la información de la institución.
3. En todos los acuerdos que impliquen la provisión de servicios en cualquier forma de contratación, que realicen dentro de la institución, se definirán los controles, requisitos de seguridad y compromisos de confidencialidad pertinentes, limitando al mínimo indispensable los permisos que se otorguen.
4. No se permitirá el acceso a la información de las instalaciones de procesamiento ni a otras áreas críticas de servicio a terceros, a menos que se cumplan los controles adecuados y/o se firme un contrato o acuerdo que defina las condiciones para el acceso o la conexión pertinente.
5. Es fundamental que los contratos y acuerdos de confidencialidad firmados con terceros incluyan cláusulas que garanticen la protección de los activos de la empresa, lo que abarca:
    a) Métodos para salvaguardar los activos de la institución, incluyendo bienes tangibles, los datos y las aplicaciones informáticas.
    b) Controles sobre la reproducción y difusión de información.
    c) Información sobre los servicios habilitados.

5.7.4.7 Gestión Seguro de Inicio de Sesión

1. Es fundamental que cada acceso exija la identificación personal del usuario a través de credenciales únicas y un proceso de autenticación seguro, evitando configuraciones que faciliten inicios de sesión automáticos sin la intervención del usuario.
2. Las sesiones activas deben cerrarse automáticamente tras un periodo de inactividad definido, para prevenir accesos no autorizados.
3. No se permite el uso de cuentas compartidas o genéricas. Es fundamental que cada individuo disponga de su propio usuario personal, asumiendo así las responsabilidades que conlleva dicha cuenta.
4. Al iniciar sesión, el sistema debe enmascarar la contraseña utilizando asteriscos y no debe exhibirla en la pantalla. Además, no se debe revelar información del sistema hasta que la autenticación sea exitosa, lo que incluye evitar mostrar nombres de usuarios existentes, detalles técnicos o mensajes de error específicos.
5. La Dirección de Seguridad Informática, junto con el Oficial de Seguridad de la información, tiene la responsabilidad de supervisar los registros de inicio de sesión para identificar accesos inusuales, múltiples intentos fallidos o comportamientos anómalos, generando alertas automáticas ante accesos sospechosos, intentos desde ubicaciones no autorizadas o accesos fuera del horario habitual.

6. El registro de un log debe permitir el seguimiento posterior de las actividades de los usuarios por ello contendrá como mínimo:
    a) Identificación del usuario
    b) Fecha y hora de inicio y finalización de sesión
    c) Dirección IP de origen y de destino
    d) Registro de ingresos que han sido exitosos y aquellos que han fallado.

5.7.4.8 Gestión de Acceso al Código Fuente de las Aplicaciones

La Dirección de Desarrollo de Soluciones Informáticas se encargará de gestionar el acceso al código fuente de los proyectos de la institución y a los elementos asociados, implementando al menos los controles siguientes:

1. Solo las personas que, debido a su rol, necesiten acceder a los programas fuente, bibliotecas y otros repositorios tendrán acceso, con el objetivo de prevenir la incorporación de funcionalidades no autorizadas y evitar modificaciones no deseadas.
2. Personal de soporte técnico no debe tener acceso a los programas fuente, bibliotecas y otros repositorios.
3. Los programas fuente, bibliotecas y demás elementos relacionados a los proyectos de la institución deben guardarse en entornos seguros, manteniendo la confidencialidad, integridad y disponibilidad de los mismos.
4. Es necesario implementar un sistema de control de versiones para los códigos fuente, asegurando que los permisos de acceso para los desarrolladores sean otorgados con la debida autorización.
5. Mantener un registro actualizado de todos los programas fuentes en uso, indicando como mínimo: el nombre del programa, el desarrollador, la persona que autoriza, la versión, la fecha de la última modificación, la fecha y hora de compilación, así como el estado (si está en modificación o en producción).

5.8. Administración de la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

5.8.1 Adquisición de Software

1. La incorporación de software o soluciones tecnológicas se llevará a cabo en función del abanico de proyectos y servicios que han sido priorizados en los planes estratégico y operativo que han sido aprobados por el área correspondiente, teniendo en cuenta lo que establece el ente regulador para la aprobación de proyectos tecnológicos. De no ser así, la máxima autoridad podrá autorizarlo, siempre que se presente una justificación técnica debidamente documentada.
2. Es fundamental adoptar, conservar y aplicar la normativa legal vigente que rige el sector tecnológico, así como los estándares internacionales en áreas como la programación de software, la nomenclatura, la experiencia del usuario, la interoperabilidad, la eficiencia del rendimiento de los sistemas, la escalabilidad, la validación de requisitos y los esquemas de pruebas unitarias e integradas.
3. Establecer y enfocar los acuerdos y requerimientos tanto funcionales como técnicos de la institución, asegurando la participación y aprobación formal de la persona encargada de la gestión de proyectos institucionales, así como de las autoridades pertinentes establecidas por la normativa vigente. Esto abarca aspectos como los tipos de usuarios y perfiles, así como los requerimientos relacionados con la entrada de datos, la definición de interfaces, el almacenamiento, el procesamiento, la salida de información, los controles, las medidas de seguridad, el plan de pruebas y los registros de auditoría para las transacciones que impliquen el registro de información.

4. Aprobación de los criterios y requisitos que definirán las necesidades, incluye su viabilidad tanto tecnológica como económica, el análisis de riesgos y el estudio de costo-beneficio, la estrategia para el desarrollo o incorporación del software, así como la gestión de los procesos de emergencia que puedan surgir.

5.8.2 Desarrollo Seguro de Soluciones Informáticas

1. Aplica a todos los desarrollos internos, contrataciones de terceros, mantenimientos evolutivos o correctivos y cualquier proceso de modificación de software que se utilice dentro del entorno institucional.
2. Desde la fase de diseño, los proyectos de soluciones informáticas deben incorporar controles de seguridad que protejan la confidencialidad, integridad y disponibilidad de la información que procesarán.
3. El personal técnico deberá aplicar estándares reconocidos de programación segura, evitando patrones vulnerables y utilizando herramientas que ayuden a detectar errores comunes en tiempo de desarrollo.
4. Los equipos de desarrollo deberán recibir formación periódica en prácticas de seguridad, nuevas amenazas y técnicas de defensa para mantener la calidad y confiabilidad del software institucional.
5. Todo desarrollo deberá pasar por revisiones técnicas que incluyan la verificación de seguridad, ya sea mediante revisión entre pares, herramientas automatizadas o pruebas específicas de vulnerabilidad.
6. Las actividades de desarrollo y pruebas deben realizarse en ambientes separados del entorno de producción. Está estrictamente prohibido probar o depurar aplicaciones directamente en sistemas operativos o bases de datos en uso.
7. Las aplicaciones deben estar programadas para manejar errores de forma controlada, sin exponer información técnica o sensible a los usuarios finales o potenciales atacantes.
8. Antes de liberar un sistema, se debe asegurar que no queden líneas de código comentadas, accesos de prueba, contraseñas embebidas u otros elementos que puedan representar un riesgo de seguridad.
9. Todo desarrollo debe ser sometido a pruebas funcionales y de seguridad antes de ser liberado. Estas pruebas deben evaluar la resistencia de la aplicación ante ataques como XSS, SQL Injection, escalamiento de privilegios, accesos indebidos o corrupción de datos.
10. Toda aplicación, ya sea desarrollada dentro de la institución o por un tercero, tendrá un responsable técnico y un funcional, con sus respectivos respaldos designados de manera formal por las direcciones correspondientes de la institución.
11. El equipo de desarrollo será el responsable de aplicar estas directrices durante todo el ciclo de vida del software.
12. El Oficial de Seguridad de la Información debe velar porque se integren controles adecuados y acompañar las validaciones necesarias.
13. Las áreas solicitantes deberán participar en la definición de requerimientos seguros y validar los resultados de las pruebas funcionales y de seguridad.

5.8.3 Mantenimiento de Soluciones Informáticas

1. Es aplicable a todo mantenimiento correctivo, adaptativo, evolutivo o preventivo que se realice sobre aplicaciones propias o de terceros en uso dentro del entorno institucional.
2. Todo trabajo de mantenimiento debe ser planificado con antelación, incluyendo una descripción clara de los cambios, responsabilidades, tiempos estimados y ventanas de intervención.
3. Ninguna modificación puede aplicarse directamente sobre el ambiente de producción sin haber pasado por el procedimiento de gestión de cambios, el cual debe contemplar pruebas previas, evaluación de impactos y aprobación formal.

4. Las intervenciones deben realizarse en entornos de desarrollo o pruebas, replicando lo más posible el comportamiento real, antes de llevarse a producción.
5. Después de cada mantenimiento se deben ejecutar pruebas que garanticen que los cambios no han generado errores colaterales ni vulnerabilidades nuevas.
6. Todo mantenimiento debe dejar evidencia clara y estructurada sobre lo que se modificó, el motivo, la persona responsable y el resultado obtenido. Esta información será parte del historial técnico de la aplicación.
7. Antes de realizar cualquier intervención, se debe generar una copia de respaldo del sistema o componente afectado, de forma que se pueda restaurar en caso de fallos.
8. Una vez aplicado el cambio, el comportamiento del sistema debe ser monitoreado durante un período prudente para detectar posibles incidencias no previstas.
9. Sólo el personal autorizado podrá realizar tareas de mantenimiento y sus actividades deberán estar registradas mediante mecanismos de auditoría.
10. La Dirección de Desarrollo de Soluciones Informáticas será la responsable de coordinar y ejecutar los mantenimientos conforme a esta política.
11. El Oficial de Seguridad de la Información deberá validar que se consideren aspectos de seguridad en cada mantenimiento significativo.
12. Las áreas encargadas del aplicativo participarán en la verificación de funcionalidades corregidas o ajustadas según sus requerimientos.

5.8.4 Licenciamiento de Software

1. Definir las directrices para el uso legal, responsable y controlado del software dentro de la institución, garantizando el cumplimiento de los marcos normativos vigentes, evitando riesgos legales, técnicos y de seguridad asociados al uso indebido o no autorizado de licencias.
2. Todo software utilizado en la institución debe contar con una licencia válida vigente y aprobada por las áreas responsables. Se prohíbe expresamente el uso de versiones piratas, no oficiales o de procedencia dudosa.
3. Se mantendrá un inventario centralizado y actualizado de todo el software licenciado, detallando tipo de licencia, proveedor, versión, fecha de adquisición, vigencia y responsable.
4. Se establecerán controles para evitar la dualidad no autorizada de licencias, su uso fuera de lo permitido por el contrato o la instalación en dispositivos no autorizados.
5. Las licencias con vigencia limitada deberán ser monitoreadas para asegurar su renovación oportuna o su desinstalación si dejan de ser necesarias o válidas.
6. No se permite duplicar total o parcialmente los códigos fuente y documentación de programas de software con derechos de propiedad intelectual, a menos que se cuente con la autorización expresa de su autor o de quien tenga los derechos.
7. Establecer y aplicar una licencia pública general al software que ha sido desarrollado por la institución o que ha sido contratado a terceros como desarrollo, para resguardar la propiedad intelectual.
8. Proteger la evidencia de la propiedad de licencias o suscripciones "open source", contratos, manuales y toda la información importante del software adquirido.

5.8.5 Instalación de Software

1. La instalación de software será autorizada únicamente cuando exista una necesidad operativa justificada y se cuente con una licencia en el caso de ser un software de paga, no se permitirán instalaciones por iniciativa personal o sin evaluación previa.
2. Se mantendrá una matriz que incluirá un listado de software autorizado para su instalación en los equipos de la institución, los cuales habrán sido previamente aprobados tras un análisis de software. Esta matriz se actualizará conforme a la demanda de software analizado.

3. Si un instalador de software, al ser evaluado, muestra un comportamiento riesgoso o tiene informes de algún malware, será incluido en una matriz conocida como lista negra. Todo software que figure en esta lista no podrá ser instalado bajo ninguna circunstancia en los equipos de la institución.
4. Los datos esenciales que debe incluir la matriz de lista blanca de software, al igual que la lista negra, son los siguientes:
    a) Nombre del software
    b) Versión
    c) Arquitectura
    d) Hash del instalador
5. Los programas que se consideran aplicaciones predeterminadas que todos los equipos de cómputo recibirán al ser entregados al usuario son los siguientes:
    a) Navegadores web (Google Chrome, Firefox, Microsoft Edge).
    b) Lector de archivos PDF (Adobe Reader).
    c) Protección de amenazas en equipos finales (EDR, XDR, etc.), sólo debe estar instalado uno por buenas prácticas y para evitar mal funcionamiento por tener varios.
    d) Herramientas de Ofimática (Word, Power Point, Excel, etc.).
    e) Herramienta de gestión de firma electrónica (FIRMAEC).
    f) Edición de PDF (PDF Gear, Nitro PDF).
    g) Comprimir archivos (WinRar)
    h) Powershell debe estar desactivado en todos los equipos.
6. Todo software que se instale debe requerir al área responsable un análisis del instalador. Este análisis puede realizarse de forma estática, dinámica o mediante ambos métodos, garantizando que el instalador sea legítimo y que su uso no cause problemas a los equipos de la institución. Una vez que se haya otorgado la autorización, se debe actualizar la matriz y proceder con la instalación en el equipo solicitado.
7. Llevar a cabo controles y auditorías con el propósito de confirmar la correcta instalación de plugins y otros complementos que podrían servir como un medio para el incumplimiento de las normas de navegación y otras restricciones establecidas mediante las herramientas de seguridad informática. Asimismo, se deberá supervisar el uso de software no recomendado por parte de los usuarios que cuenten con permisos excepcionales de administración local en sus dispositivos. En ambos casos, cualquier infracción deberá ser reportada al Oficial de Seguridad de la Información para gestionar la sanción correspondiente a través de la Gerencia de Talento Humano.

5.9. Administración de Reporte de Incidentes de Seguridad de la Información

1. Todo usuario debe estar atento a posibles señales de incidentes, como accesos no autorizados, archivos inusuales, comportamiento anómalo del sistema, filtración de información, fallos inesperados o actividades sospechosas.
2. Ante la sospecha o evidencia de un incidente, se debe reportar de forma inmediata al equipo de soporte técnico o al Oficial de Seguridad de la Información, sin intentar resolverlo por cuenta propia.
3. Cada incidente debe quedar documentado en un registro central, indicando fecha, hora, descripción, sistemas afectados, nivel de impacto, acciones tomadas y responsabilidad del reporte.
4. Los incidentes serán analizados para determinar su naturaleza (por ejemplo, intento de intrusión, pérdida de datos, ataque de malware, suplantación de identidad, etc.), su alcance y posibles causas.
5. Se aplicarán medidas técnicas y organizativas de manera oportuna para contener el incidente, evitar que se propague o agrave y restaurar los servicios afectados con el menor impacto posible.
6. Cuando el incidente lo amerite; por su gravedad, alcance o normativa legal, se informará a las autoridades competentes y a los entes reguladores según lo establecido en el marco legal vigente.

7. Cada incidente debe ser aprovechado como una oportunidad para aprender y reforzar el sistema de gestión. Se evaluarán causas raíz, se establecerán acciones correctivas y se actualizarán controles de seguridad si es necesario.
8. Toda la información relacionada con la investigación y resolución de incidentes será tratada con estricta confidencialidad, limitando su acceso solo a las personas involucradas en su análisis y gestión.
9. El Oficial de Seguridad de la Información liderará la gestión de los incidentes, asegurando a su análisis, seguimiento y cierre conforme a los procedimientos establecidos.
10. La Dirección de Seguridad Informática deberá brindar soporte técnico inmediato y participar en la contención y recuperación.
11. Todos los servidores están obligados a reportar cualquier hecho anómalo relacionado con la seguridad de la información y seguir las instrucciones correspondientes.

5.9.1 Del manejo de Incidentes relacionados con la Seguridad de la Información

El Oficial de seguridad de la información será responsable de desarrollar y gestionar la aprobación del procedimiento detallado para la gestión de incidentes, el cual incluirá al menos lo siguiente:

1. Análisis de eventos y determinación de incidentes.
2. Evaluación de incidentes, diagnóstico, eventos ocurridos, impactos y análisis de causa raíz.
3. Escalabilidad de incidentes y tipos de soluciones.
4. Investigaciones a realizar y fuentes de información que se utilizarán.
5. Mejora y/o fortalecimiento de controles internos en el ámbito de la seguridad de la información.
6. Elaboración de informes y/o respuestas ante incidentes.
7. Monitoreo de la respuesta implementada o ejecutada para resolver el incidente.
8. Creación de una base de conocimiento sobre los incidentes de Seguridad de la Información y su tratamiento correspondiente.
9. Toda la información generada a partir de incidentes será considerada confidencial y se establecerán niveles de accesibilidad para las autoridades y organismos de control.

5.10. Gestión, Supervisión y Auditoría

1. Se implementarán mecanismos de seguimiento constantes sobre los sistemas críticos, con el fin de identificar accesos indebidos, comportamientos anómalos, fallas o desviaciones de las políticas de seguridad.
2. Las actividades de control se realizarán de manera periódica y planificada, cubriendo tanto aspectos técnicos (accesos, configuraciones y eventos de seguridad) como organizativos (cumplimiento de roles, procedimientos y responsabilidades).
3. Se ejecutarán auditoría interna con frecuencia establecida, evaluando el grado de cumplimiento de los controles, la efectividad de las medidas implementadas y la adherencia a las normativas institucionales y legales aplicables.
4. Cuando corresponda por normativa o decisión institucional se podrán realizar auditorías externas por parte de entes reguladores o auditores especializados, asegurando la objetividad del proceso.
5. Todas las actividades relacionadas con control. Seguimiento y auditoría deberán quedar documentadas, incluyendo hallazgos, responsables, tiempo y evidencias. Esta información servirá como base para acciones de mejora o correctivas.
6. El personal involucrado en auditorías y revisiones tendrá acceso a la información necesaria, respetando los principios de confidencialidad, integridad y uso legítimo de los datos.
7. Los resultados obtenidos de los procesos de control y auditoría serán analizados para definir ajustes o refuerzos en los controles existentes. Toda observación relevante será tratada a través de planes de acción documentados y con responsables asignados.
8. El Oficial de Seguridad de la Información tiene la responsabilidad de coordinar los procesos de seguimiento y auditoría.

9. Las áreas responsables de los procesos deben participar de manera activa en los controles y en la ejecución de mejoras.
10. La Coordinación Técnica de Innovación Tecnológica tendrá a su cargo el monitoreo de sistemas técnicos y la generación de reportes de seguridad.

5.11. Gestión de la Continuidad del Negocio

1. Se deben identificar y priorizar los procesos, servicios y activos de información cuya interrupción pueda causar un impacto significativo en el cumplimiento de los objetivos institucionales.
2. Se realizará un Análisis de Impacto (BIA) al negocio que permita determinar las consecuencias potenciales de una interrupción, así como los tiempos máximos aceptables para su recuperación.
3. Se analizarán los riesgos asociados a la indisponibilidad de recursos, fallas técnicas, desastres naturales, ataques cibernéticos o cualquier otra amenaza que afecte la continuidad.
4. La institución debe contar con planes actualizados que contemplen acciones preventivas, procedimientos de contingencia y mecanismos de recuperación, tanto para procesos como para sistemas tecnológicos.
5. Los planes de continuidad serán verificados mediante pruebas periódicas y simulacros, para evaluar su efectividad, medir los tiempos de respuesta y realizar los ajustes necesarios.
6. Se definirá un equipo responsable de gestionar la continuidad del negocio, incluyendo roles claros para la toma de decisiones, la comunicación en crisis y la ejecución de planes de recuperación.
7. El personal involucrado será capacitado en sus responsabilidades durante una contingencia, asegurando que conozcan los procedimientos a seguir en caso de interrupciones o emergencias.
8. Los planes y procedimientos de continuidad deben revisarse y mejorarse de manera periódica o tras la ocurrencia de un evento relevante, para incorporar lecciones aprendidas y adaptarse a nuevos escenarios de riesgos.

5.12. Protección de Datos Personales

1. Solo se recolectará y procesará la información estrictamente necesaria para cumplir con los fines institucionales. No se deberá almacenar ni utilizar datos innecesarios o excesivos.
2. El acceso a datos será controlado según el rol, la necesidad funcional y el principio de mínimo privilegio. Ningún usuario deberá acceder a información para la cual no tenga autorización expresa.
3. Toda la información considerada sensible, clasificada o confidencial deberá ser tratada bajo estrictas medidas de seguridad y no podrá ser compartida sin una autorización formal.
4. En los casos que así lo exijan las normativas sobre protección de datos personales, se deberá contar con el consentimiento expreso de los titulares antes de recolectar, tratar o compartir su información.
5. En los casos que así lo exijan las normativas vigentes sobre protección de datos personales, se deberá contar con el consentimiento expreso de los titulares antes de recolectar, tratar o compartir su información.
6. La institución informará de manera clara y oportuna a los titulares de datos sobre el uso que se dará a su información, el tiempo de conservación y los derechos que pueden ejercer.
7. Se implementarán controles técnicos y organizativos como cifrados, autenticación robusta, copias de seguridad, gestión de accesos, entre otros, para proteger los datos durante todo su ciclo de vida.
8. Cada persona con acceso a datos institucionales es responsable de su buen uso y manejo adecuado, siguiendo las políticas internas y actuando con diligencia.
9. La institución garantizará que los titulares puedan ejercer sus derechos de acceso, rectificación, actualización, eliminación o revocatoria del consentimiento conforme lo establecido en la ley.
10. Si por necesidad operativa se deben compartir datos con terceros, se establecerán acuerdos que aseguren su tratamiento adecuado y la protección de la información transmitida.

6. INCUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

El no cumplimiento de estas Políticas de Seguridad de la Información dará lugar a las sanciones pertinentes de acuerdo con lo establecido por la normativa institucional, sin menoscabo de las otras acciones legales (administrativas, civiles y/o penales) que correspondan según la legislación vigente.

7. GLOSARIO Y ACRÓNIMOS.

7.1. Glosario

Tabla 7.1 Palabras de glosario

Palabra(s)	Descripción
Activos de información	Cualquier recurso (datos, hardware, software, personas, servicios) que tenga valor para una institución pública y deba protegerse.
Amenaza	Causa potencial de un incidente no deseado que puede dañar los activos de información.
Análisis de Riesgos	Proceso para identificar, evaluar y priorizar riesgos sobre los activos de información.
Autenticación	Proceso de verificar la identidad de un usuario o sistema.
Administración de la Continuidad	Es un proceso permanente que garantiza la continuidad de las operaciones del negocio a través de la efectividad del mantenimiento del plan de continuidad.
Antivirus	Es un programa de seguridad informática diseñado para detectar, prevenir y eliminar software malicioso, conocido como malware, que puede dañar un dispositivo o comprometer la seguridad del usuario.
Cifrado	Es el proceso de convertir información legible (texto plano) en un formato ilegible (texto cifrado) para ocultar su contenido a usuarios no autorizados.
Cookies	Son pequeños archivos de texto que un sitio web guarda en el navegador de un usuario para recordar información sobre su visita o comportamiento en la web.
Clasificación de la información	Proceso de etiquetar la información según su nivel de sensibilidad (Pública, Interna, Confidencial, Reservada).
Confidencialidad	Garantía de que la información solo esté disponible para quienes tienen autorización.
Controles de seguridad	Medidas (técnicas, físicas o administrativas) implementadas para reducir los riesgos.
Disponibilidad	Asegurar que la información esté accesible cuando se la necesite.
Evaluación de riesgos	Resultado del análisis de riesgos, incluye el nivel de riesgo residual y las medidas propuestas.
Gestión de incidentes	Proceso para identificar, reportar, responder y aprender de eventos de seguridad.
Gestión de vulnerabilidades	Identificación, evaluación y tratamiento de debilidades en los sistemas.
Integridad	Garantía de que la información no ha sido modificada de manera no autorizada.

Ingeniería Social	Es una técnica de manipulación que aprovecha el error humano para obtener información privada, acceso o bienes valiosos.
Inventario de Activos	Registro documentado de todos los activos que deben ser protegidos.
Hardening	Endurecimiento de un sistema, es el proceso de aumentar la seguridad de un sistema informático o red, reduciendo su superficie de ataque y minimizando vulnerabilidades.
Malware	Abreviatura de "malicious software" o "software malicioso", es cualquier programa o código informático diseñado intencionalmente para causar daño o interrupciones en un sistema informático, como computadoras, servidores, clientes o redes.
Matriz de Riesgos	Herramienta visual que ayuda a categorizar riesgos según impacto y probabilidad.
Passphrases	Frase de contraseña, es una secuencia de palabras, normalmente más larga que una contraseña tradicional, utilizada para autenticar o asegurar el acceso a un sistema, aplicación o cuenta en línea.
Política de seguridad de la información	Declaración formal del compromiso institucional con la seguridad de la información.
PDF	Portable Document Format es un formato de archivo que permite mostrar documentos de forma electrónica de manera independiente del software, hardware o sistema operativo utilizado.
Phishing	Es una técnica de ciberdelincuencia que utiliza el engaño para robar información confidencial de las víctimas.
Plugings	Es un software adicional que se instala en un programa principal para añadir nuevas funcionalidades o mejorar las existentes.
Ransomware	Es un tipo de software malicioso (malware) que bloquea el acceso a los archivos, sistemas o redes de una computadora y exige el pago de un rescate para recuperarlos.
Requisitos mínimos de seguridad (RMS)	Controles que deben aplicarse obligatoriamente en cada entidad.
Riesgo	Combinación de la probabilidad de un evento y su impacto negativo en los activos de información
Root	Se refiere al usuario con privilegios de administrador, que tiene acceso total a todo el sistema de archivos.
SQL Injection	Es un método de infiltración de código intruso que se vale de una vulnerabilidad presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.
Seguridad de la Información	Protección de la información contra accesos, usos o modificaciones no autorizadas.
Spyware	Es un tipo de malware que se instala en un dispositivo (como una computadora, un teléfono inteligente o una tableta) sin el conocimiento o consentimiento del usuario.
SSH	Significa Secure Shell, es un protocolo de red que permite acceder de forma segura a un servidor o máquina remota a través de una conexión cifrada.

Telnet	Es un protocolo de red que permite a los usuarios interactuar con máquinas remotas a través de una conexión de terminal virtual.
Tratamiento del Riesgo	Proceso para seleccionar e implementar medidas que reduzcan los riesgos.
Troyano	Malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.
XDR	Detección y respuesta extendidas (Extended Detection and Response). Es un enfoque de ciberseguridad que recopila y correlaciona datos de seguridad de diferentes fuentes, como endpoints, redes, correo electrónico y nube, para mejorar la detección y respuesta a las amenazas.
XSS	Cross-Site Scripting, es una vulnerabilidad de seguridad en aplicaciones web que permite a los atacantes inyectar código malicioso en páginas web legítimas para comprometer las interacciones de los usuarios.
VPN	Red Privada Virtual (Virtual Private Network), es una tecnología que permite crear una conexión segura y encriptada entre tu dispositivo y un servidor remoto.

7.2. Acrónimos

Tabla 7.2 Acrónimos

Palabra(s)	Descripción
BRP	Business Resumption Planning (Plan de Recuperación Empresarial)
BIA	Business Impact Analysis (Análisis de Impacto en el Negocio)
DRP	Disaster Recovery Plan (Plan de Recuperación ante Desastres)
EGSI	Esquema Gubernamental de Seguridad de la Información
IOC	Indicadores de Compromiso
PAM	Privileged Access Management (Gestión de Accesos Privilegiados)
SaaS	Software como Servicio
SGIS	Sistema de Gestión de Seguridad de la Información

8. ANEXOS.

No aplica.

8.1. FIRMAS DE ELABORACIÓN Y APROBACIÓN

	Nombre/ Cargo	Firma
Elaborado por:	Ítalo Fernando Parreño Sañicela Oficial de Seguridad de la Información	Firmado electrónicamente por: ITALO FERNANDO PARRENO SANICELA Validar únicamente con FirmaEC
Revisado por:	Nataly Patricia Avilés Pastás Presidenta del Comité	Firmado electrónicamente por: NATALY PATRICIA AVILES PASTAS Validar únicamente con FirmaEC
Aprobado por:	José Julio Neira Hanze Director General, Encargado	Firmado electrónicamente por: JOSE JULIO NEIRA HANZE Validar únicamente con FirmaEC