POLÍTICA DE DESARROLLO SEGURO

1. Objetivo Establecer los lineamientos y buenas prácticas para el desarrollo seguro de aplicaciones web en VB .NET, PHP, JAVA, JavaScript entre otras, con el fin de garantizar la ciberseguridad, proteger la información y los datos de la empresa y prevenir vulnerabilidades que puedan comprometer los sistemas corporativos.

2. Alcance Esta política aplica a todos los desarrollos web realizados en VB .NET por el equipo de Tecnologías de la Información, incluyendo nuevos proyectos, mantenimiento de aplicaciones existentes y/o actualizaciones que se realicen a partir de la fecha de entrar en vigencia esta política.

El Acueducto Metropolitano de Bucaramanga S.A. E.S.P., en cumplimiento de los lineamientos establecidos en el Decreto 1078 de 2015 y sus modificaciones y del Decreto 338 de 2022, adoptará prácticas de desarrollo seguro en todas las aplicaciones web y sistemas de información que diseñe o contrate, garantizando la implementación de controles que aseguren la confidencialidad, integridad, disponibilidad y trazabilidad de la información durante todo el ciclo de vida del software, conforme con los estándares definidos por el Ministerio TIC.

3. Definiciones

Para los propósitos de este documento se aplican los siguientes términos y definiciones:

Activo: Cualquier bien que tenga valor para la organización.

• Acuerdo de Confidencialidad: Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de La Cámara de Comercio.

• Administradores: Usuarios a quienes la Cámara de Comercio ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos de la Cámara de Comercio quienes estarán bajo la Dirección de tecnología de la información.

• Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

• Backup: Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.

• Comité de Seguridad de la información y protección de datos personales: Equipo de trabajo conformado por la resolución de creación del comité.

• Contraseña: Clave de acceso a un recurso informático.

• Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

• Directrices: Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los

objetivos establecidos en las políticas.

• Servicios de procesamiento de información: Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.

• Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

• Evento de seguridad de la información: Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

4. Principios Generales

4.1 Confidencialidad, Integridad y Disponibilidad: Los desarrollos deben garantizar que la información se mantenga protegida contra accesos no autorizados, alteraciones indebidas y estar disponible para los usuarios autorizados.

- **Garantizar**: Establecer controles de acceso estrictos para las aplicaciones y bases de datos.
- Implementar cifrado de datos en tránsito con certificados (SSL) y en reposo.
- Implementar cifrado de datos enviados por correo electrónico a través del estándar (TLS 1.2 como mínimo).
- Diseñar pruebas de estrés y recuperación para asegurar la disponibilidad.
- Establecer un contrato de mantenimiento y actualización del software durante la vida útil del proyecto.

4.2 Cumplimiento Normativo: Asegurar que los desarrollos cumplan con las leyes y regulaciones aplicables, como lo son la Ley 1273 de 2009 (Ley de Delitos Informáticos), Decreto 338 de 2022 (Seguridad Digital), Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones) e incluyendo la ley 1581 de 2012 normativa de protección de datos personales.

- **Garantizar**: Revisar los desarrollos contra una lista de control de cumplimiento (checklist) basada en regulaciones como la Ley de Protección de Datos Personales.
- **Medir**: Cantidad de incidentes de incumplimiento a políticas de desarrollo seguro, detectados o reportados, lo cual será documentado en la bitácora de incidentes.

4.3 Prevención de Vulnerabilidades: Implementar medidas para prevenir ataques como inyección SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), entre otros.

5. Lineamientos para Desarrollo Seguro

5.1 Diseño Seguro

- Seguir principios de mínimo privilegio, asegurando que las aplicaciones otorguen solo los

accesos necesarios a los usuarios.
- Adoptar una arquitectura de defensa en profundidad para proteger los datos sensibles.
- Cuando se elija la plataforma o leguaje debe ser la última versión estable.
- El framework en el cual se desarrolle, debe ser el último estable que sea compatible con la infraestructura del amb.
- Si el diseño contiene recepción de archivos, este traslado de archivo se debe hacer a través de API´s de envío (desde la zona DMZ) y recepción (servidores internos) en la disposición final.
- En el diseño se debe requerir el apagado y encendido sencillo de la aplicación sin necesidad de apagar servicios en los servidores.
- Si el software contiene base de datos, este manejador de base de datos debe ser SQL Server. Cabe las excepciones donde ya el producto tenga su propio base de datos ya definido y este no se pueda cambiar, caso en el cual el contratista debe entregar el licenciamiento del motor de base de datos a nombre del Acueducto Metropolitano de Bucaramanga S.A. ESP.
- Se debe contemplar la gestión riesgos de seguridad digital, tener planes de seguridad, respuesta a incidentes, y garantizar la integridad, disponibilidad y confidencialidad de sistemas.

5.2. Codificación Segura

- Validar y sanitizar todas las entradas de usuario para prevenir inyecciones y otros ataques.
- Usar conexiones parametrizadas para evitar inyección SQL.
- Implementar controles de autenticación y autorización robustos. Como captcha o rutinas que impidan el uso de robots y con doble factor de autenticación.
- Las contraseñas de los usuarios tienen que ser codificadas o encriptadas en las tablas de base de datos.
- Evitar el almacenamiento de información sensible en texto claro; utilizar mecanismos de cifrados seguros.
- Manejar las excepciones de manera adecuada, evitando exponer información sensible en mensajes de error.

5.3. Pruebas de Seguridad

Se realizarán anualmente ejercicios de Hacking Ético aleatoriamente a las aplicaciones web para detectar vulnerabilidades, a través de las siguientes pruebas:

- Realizar pruebas estáticas y dinámicas de seguridad para identificar vulnerabilidades en el código.
- Implementar pruebas de penetración regulares para evaluar la seguridad de las aplicaciones.
- Corregir o mitigar las vulnerabilidades identificadas.

5.4. Mantenimiento Seguro

- Actualizar periódicamente las bibliotecas y dependencias utilizadas en los desarrollos para proteger contra vulnerabilidades conocidas.
- Monitorear las aplicaciones en producción para detectar posibles incidentes de seguridad.
- Establecer un proceso para gestionar incidentes de seguridad, incluyendo la notificación,

contención y resolución.
- La aplicación debe tener apagado seguro desde el mismo aplicativo con el fin de hacer mantenimientos.

5.5 Política para aplicaciones web en VB .NET, PHP, JAVA, JavaScript entre otras

El Área de Tecnologías de la Información realizará anualmente un ejercicio de Hacking Ético con el fin de evaluar el cumplimiento de la Política de Desarrollo Seguro, identificar vulnerabilidades y verificar la actualización de los desarrollos a las versiones más recientes de sus componentes y frameworks.

Todo contrato o proyecto de desarrollo de software, ya sea interno o externo, deberá incluir las actividades necesarias para mitigar las vulnerabilidades identificadas durante dicho ejercicio anual, garantizando así la mejora continua y la seguridad de las aplicaciones web utilizadas por el amb.

6. Roles y Responsabilidades

Desarrolladores:

- Implementar las buenas prácticas de desarrollo seguro descritas en esta política.
- Establecer planes y actividades relacionados con la seguridad de la información
- Adelantar las acciones del plan de sensibilización de la política de seguridad de la información
- Realizar las revisiones y actualizaciones pertinentes de manera periódica de la política de seguridad de la información y socializar.

Jefes de Proyecto:

- Asegurar que los desarrollos cumplan con los lineamientos de seguridad antes de su despliegue.
- Comunicar a todos los colaboradores de la empresa en cada una de sus áreas la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y las necesidades de la mejora continua, como parte de la estrategia del *amb S.A E.S.P.*

- Documentar los procedimientos que sean requeridos en el marco de la seguridad de la información.

Equipo de Seguridad:

- Proveer capacitación, herramientas y soporte necesarios para garantizar el cumplimiento de esta política.
- Realizar la planeación de auditoría internas relacionadas con los sistemas de gestión integrados que se encuentren implementadas.

Usuarios Finales:

- Reportar cualquier comportamiento anómalo en las aplicaciones.

7. Capacitación y Concientización El personal involucrado en el desarrollo de aplicaciones web recibirá capacitación regular en buenas prácticas de desarrollo seguro y en el manejo de herramientas de seguridad.

8. Revisión y Actualización Esta política será revisada anualmente o cuando surjan cambios significativos en las tecnologías, amenazas o regulaciones que la afecten así lo ameriten, a fin de asegurar siempre su oportunidad, idoneidad, completitud y precisión.

9. Cumplimiento. El incumplimiento, violación u omisión a la Política de Desarrollo Seguro del *amb S.A E.S.P.* traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas disciplinarias de acuerdo con las normas internas de la empresa.

Todos los trabajadores de la empresa, así como los contratistas, deben cumplir y acatar el manual de política de seguridad de la información en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento de los gerentes y jefes de cada área, a través de la inclusión de esta obligación en el manual de funciones y las cláusulas contractuales.

10. Seguimiento y Evaluación

Se debe garantizar un contrato de mantenimiento de los desarrollos con el fin de corregir problemas de obsolescencia de software y las vulnerabilidades que surjan de ejercicio de Hacking Ético de la empresa.

11. Cultura en Seguridad

El *amb S.A E.S.P.* debe velar por la apropiación y el fortalecimiento de una cultura de Seguridad y Privacidad de la Información adecuada, por lo cual implementará las medidas requeridas y necesarias para sensibilizar y concientizar a los trabajadores, contratistas y partes interesadas de manera continua.

12. Publicación

La presente política se emite mediante de Acto de Gerencia y se publicará en la Página Web y la Intranet del Acueducto Metropolitano de Bucaramanga S.A. E.S.P. y se trasladará a los Gerentes de Área, Lideres de Área, Lideres de procesos 2 y 3, para su general divulgación y aplicación, así como a las Áreas de Gestión Humana y Control de Gestión para la aplicación de las disposiciones que son de su competencia.

Esta política será difundida por el Área de TI por medio de correos electrónicos, notas informativas de prensa, publicaciones y charlas a los trabajadores nuevos y desarrolladores de software para asegurar una comprensión integral y la adopción de las medidas de seguridad contempladas en esta política.

13. vigencia.

La presente Política rige a partir de la fecha de su expedición y deroga todas las disposiciones anteriores que han sido objeto de modificación, así como aquellas que el sean contrarias.

Para constancia firma,

DARIO GIOVANNI LIZCANO BENITEZ
Primer Suplente del Gerente General

Elabora: TIC´s
Revisó; JGarcia Líder Area TIC
2025-11-04

Revisa: SG

2025-11-05