1. OBJETIVO:

Brindar lineamientos necesarios para tener en cuenta en la fase de desarrollo de Software, que brinde mecanismos y controles de seguridad para Comunicaciones Empresariales de Colombia S.A.S.

2. ALCANCE:

Proveer los lineamientos y/o directrices referentes a la Seguridad de la Información y a sus pilares de integridad, disponibilidad y confidencialidad que se requiere con el fin de llevar a cabo la planeación, desarrollo, implementación, y demás actividades necesarias para el correcto desarrollo software.

3. DEFINICIONES

Certificación: transición del requerimiento solo si se requiere de una certificación por parte de un ente externo.

Cliente: Líder Funcional o usuario experto que tiene amplio conocimiento y manejo de los aplicativos de software administrados por CEM.

Mejora: proceso de cambio o implementación de nueva solución o desarrollo de Software.

Desarrollo: Conjunto de componentes lógicos necesarios, para hacer posible la realización de tareas específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido, con especial énfasis en los negocios, facilitando la interacción entre los componentes físicos, el resto de las aplicaciones, proporcionando una interfaz con el usuario.

Pruebas Funcionales: Pruebas que certifiquen el correcto funcionamiento del desarrollo según lo requisitos solicitados.

Pruebas Unitarias: Pruebas que certifiquen el correcto funcionamiento del desarrollo, para comprobar si son correctos las piezas de código individuales.

Requerimiento: Una solicitud de servicio tipificada como requerimiento; es una necesidad expresada y documentada por el cliente sobre el contenido, forma o funcionalidad de un producto o servicio.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas**.**

Sprint: Es el período en el cual se lleva a cabo el trabajo en sí.

Verificación: confirmación mediante la aportación de evidencia objetiva, donde se valida el cumplimiento de las especificaciones definidas, esta comprende acciones tales como:
- Elaboración de cálculos alternativos;
- Comparación de la especificación de un diseño nuevo, con un diseño similar probado.
- Realización de ensayos, pruebas y demostraciones.
- Revisión de documentos antes de la salida a producción.

Front: Termino en Ingles que traduce al frente

Back: Termino en Ingles que traduce detrás o al respaldo

4. SEGURIDAD EN EL DESARROLLO DE SOFTWARE

4.1. Control de acceso a la aplicación con autenticación simple:

4.1.1. Debe tener un control ante fallo de autenticación (límite de intentos de validación, bloqueo/desbloqueo de inicio de sesión)

4.2. Gestión de usuarios y gestión de privilegios:

4.2.1. Se debe incluir vigencia de activación de la cuenta de usuario (fecha de creación, periodos de suspensión).

4.3. En caso de que la aplicación sea web, sin que los otros ítems de la presente guía sean excluyentes en cuánto apliquen, se debe considerar:

4.3.1. El uso de protocolo SSL – HTTPS.
4.3.2. Procurar que el uso de cookies sea mínimo y se usen solo si es necesario, en caso de que éstas se usen se recomienda que estén cifradas.
4.3.3. Las URL deben ser limpias, es decir no exponer las variables del código en el enlace.
4.3.4. Tener en cuenta buenas prácticas de desarrollo como el top10 de OWASP.
4.3.5. Controles contra inyección de código: límite y validación de campos, codificación de caracteres especiales:
4.3.5.1. Controles de gestión de sesión y autenticación.

4.3.5.2. Controles para evitar el “Cross Side Scripting” (XSS): límite y validación de campos, codificación de caracteres especiales. Si se maneja información de alto nivel sensible o confidencial, es recomendable incluir en la validación de código HTML el uso de listas blancas (negar todo lo que no esté expresamente permitido).

4.3.5.3. Configuración de seguridad incorrecta: evitar configuraciones por defecto asegurar una arquitectura con una separación a nivel de Seguridad optima y eficiente para los componentes.

4.3.5.4. Exposición de datos sensibles: en pro de proteger la información, eliminar información innecesaria y deshabilitar la función de autocompletar e inhabilitar cache en los formularios que manejen información sensible.

4.3.5.5. Control de acceso inexistente a funciones específicas: se deben eliminar accesos y funciones por defecto, así como también gestionar los accesos y autorizaciones para el uso.

4.3.5.6. Falsificación de peticiones en sitios cruzados (CSRF): para evitar que los usuarios sean víctimas de peticiones HTML no autorizadas o que se ejecuten funciones que afecten la integridad de la información, se pueden implementar controles como: captcha, token en url, o reconfirmación de datos (ej: ¿Está seguro que desea enviar los datos del formulario? Sí/No).

4.3.5.7. Uso de componentes con vulnerabilidades conocidas: no utilizar funciones no actualizadas

4.3.5.8. En el caso de reenviar información a otras páginas o direcciones URL, verificar que no se expongan los parámetros o que estos no sean modificables en la transmisión de dicha información.

4.4. Para el Uso de formularios, se debe considerar:

4.4.1. Validación de campos y validación de datos de entrada.

4.4.2. Límite del número de caracteres permitidos.

4.4.3. Si existe interacción entre usuarios públicos (internet) y la aplicación y se requiere el envío de información y registro de correo electrónico se debe implementar control Captcha 2.0 o superior.

4.4.4. Utilizar en el formulario controles para la validación de parámetros en el campo de email, para evitar el almacenamiento en base de datos de “información borrador” o “información basura”.

4.4.5. El envió de datos del formulario debe ser método post (oculto en el código). Recomendaciones a nivel de estructuración de código: - No se deben "quemar" (Dejar contraseñas escritas en el código) contraseñas y usuarios dentro del código. Al igual que direccionamiento IP interno, en el caso de páginas web.

4.4.6. Evitar las saturaciones de buffer.

4.4.7. Es recomendable eliminar las notificaciones de error que notifican sobre los servicios o tecnología usada. Se pueden realizar pruebas de inserción de errores para verificar la respuesta de la aplicación ante un error forzado.

4.5. Se debe procurar que las páginas o portales muestren mensajes relacionados con la propiedad intelectual, protección de datos personales, privacidad y transparencia.

4.6. Auditoria y Logs - La aplicación debe almacenar registros automáticos de los cambios y acciones realizadas por usuarios en la aplicación, estos logs deben ser gestionables y deben estar protegidos y en lo posible ser no editables.

5. ROLES Y RESPONSABILIDADES

Arquitecto Senior TI/ Director Arquitectura TI/ Desarrolladores/ Documentadores/ Testing :	• Garantizar la implementación del presente estándar en la creación de cualquier software al interior de la compañía.
Seguridad de la Información:	• Velar y definir los lineamientos para el cumplimiento de este estándar y su política relacionada.

6. VERIFICACIÓN DE CUMPLIMIENTO

- El área de Seguridad de la Información realizará inspecciones como mínimo anualmente para validar el cumplimiento de los lineamientos indicados en este documento.
- La Dirección de Auditoría de la compañía deberá realizar como mínimo una auditoría en el periodo de un año y en cualquier momento podrán adelantar inspecciones sobre los servidores, dispositivos de red, aplicaciones y equipos de cómputo para corroborar el acceso de los usuarios autorizados y los lineamientos indicados en este estándar y su política relacionada.

- Durante el ciclo de Auditorías Internas del Sistema de Gestión se revisará el cumplimiento de los controles definidos en este documento.

7. ACTUALIZACIÓN

Este documento será modificado de acuerdo con las necesidades de la Organización y de las áreas implicadas en el momento que se requiera y será divulgado a las partes interesadas.

La revisión de la vigencia de las directrices se realizará mínimo una vez cada año.

8. CONTROL DE INFORMACIÓN DOCUMENTADA

Documentos que permiten verificar el cumplimiento de este estándar:

- SIGO-SI-11.0-GSI-POL Desarrollo Seguro.

Ver SIGO-CDR-LM-01 Listado maestro de información Documentada.

El mantenimiento de registros será de suma importancia por razones de contabilidad, auditoría y otras pertinentes a gestión.

9. APROBACIÓN DEL ESTANDAR

Esta estándar es aprobado por la alta dirección en la figura del Representante Legal

Representante Legal

Comunicaciones Empresariales de Colombia SAS