OBJETIVO

Definir y establecer los lineamientos y actividades para el desarrollo de software y sistemas en la empresa.

ALCANCE

Aplica a todos las áreas, colaboradores y terceros relevantes que formen parte o brinden servicios a la empresa.

POLÍTICA DE DESARROLLO SEGURO

- La empresa velará porque el desarrollo interno o externo de software y sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de sistemas de información, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuente con el nivel de soporte requerido por la institución.
- En la evaluación de riesgos de seguridad de la información realizada según la metodología de gestión de riesgos de la empresa, el Oficial de Seguridad de Información debe considerar lo siguiente:
  - Los riesgos relacionados con el acceso no autorizado al ambiente de desarrollo.
  - Los riesgos relacionados con los cambios no autorizados sobre el ambiente de desarrollo.
  - Las vulnerabilidades técnicas de los sistemas utilizados en la institución.
  - Los riesgos que puede traer una nueva tecnología si se utiliza en la institución.
- Se debe asegurar el ambiente de desarrollo, identificando lo siguiente:
  - Accesos lógicos al ambiente de desarrollo para personal de la organización.
  - Accesos lógicos al ambiente de desarrollo para personal externo.
  - Separación lógica de los ambientes de desarrollo, prueba y producción.
  - Realización de copias de respaldo de los ambientes de desarrollo.
- Se debe utilizar y aplicar los siguientes principios de ingeniería de sistemas seguros:
  - Partir siempre de un modelo de permisos mínimos, es mejor ir escalando privilegios por demanda de acuerdo a los perfiles establecidos en el ciclo de vida del software.
  - Asegurar de limpiar el código que se pone en producción, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido.
  - Nunca confiar en los datos que ingresan a la aplicación, todo debe ser validado para garantizar que lo que está ingresando a los sistemas es lo esperado y además para evitar inyecciones externas de código.
  - Hacer un seguimiento de las tecnologías utilizadas para el desarrollo. Estas van evolucionando y cualquier mejora que se haga puede dejar obsoleta o inseguras versiones anteriores.

Elaborado por:	Revisado por:	Homologado por:	Aprobado por:
Julius K. Villavicencio Monti – **Oficial de Seguridad de la Información**	Jorge Herbozo – **Líder de Gobierno Digital**	**Departamento de Planeamiento y Control de Gestión**	Juan Carlos Febres Teves - **Gerente General**
Firma: Firmado digitalmente por: VILLAVICENCIO MONTI Julius Korol FAU 20425809882 hard Fecha: 09/06/2021 16:30:35	**Firma:** Firmado digitalmente por: HERBOZO PEREZ COSTA Jorge Luis Pelayo FAU 20425809882 hard Fecha: 09/06/2021 11:50:42	**NO APLICA**	**Firma:** Firmado digitalmente por: FEBRES TEVES Juan Carlos FAU 20425809882 hard Fecha: 09/06/2021 19:00:59

  - Todos los accesos exitosos y/o fallidos que se hagan a los sistemas deben ser registrados en los logs de auditoría.
  - Se debe evaluar las transacciones sensibles en los sistemas de información para considerar que se incluyan dichas transacciones en los logs de auditoría.
  - Cualquier funcionalidad, campo, botón o menú nuevo debe agregarse de acuerdo a los requerimientos. De esta forma se evita generar código que resulte siendo innecesario.
  - La información almacenada en dispositivos móviles debería ser la mínima, y más si se trata de contraseñas o datos de sesión. Este tipo de dispositivos son los más propensos a ser que se pierdan y por lo tanto su información puede ser expuestas más fácilmente.
  - Cualquier cambio que se haga debería quedar documentado, esto facilitará modificaciones futuras.
- Todo requisito o cambio debe ser realizado de acuerdo al procedimiento establecido por la institución y debe considerar temas relacionados a seguridad de la información.
- Los propietarios de los sistemas de información son responsables de asegurarse que se realicen las pruebas para asegurar que se cumplan con los requerimientos de seguridad establecidos antes del pase a producción de los sistemas y aprobando los pases a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los sistemas de información.
- La Oficina de Tecnologías de la Información y Comunicaciones debe asegurar y cumplir lo siguiente:
  - Deberá implantar los controles necesarios para asegurar que las instalaciones y/o actualizaciones al ambiente de producción han sido aprobadas.
  - Deberá asegurase que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
  - Deberá asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
  - Deberá asegurar que el código fuente del software y/o sistemas de información se encuentre almacenado en un lugar apropiado y debe limitar el acceso lógico solamente a personal de desarrollo.
  - Deberá supervisar de manera periódica los niveles de acceso y perfiles a los ambientes de desarrollo, pruebas y producción.
  - Deberá capacitar de manera periódica, o cuando se requiera, al personal de desarrollo, pruebas y producción en temas relacionados a desarrollo seguro de software y sistemas de información.

- Los desarrolladores deben asegurar y cumplir lo siguiente:
  - Deberán considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el análisis hasta la puesta en marcha.
  - Deberán proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software y/o sistemas de información; dicho soporte debe contemplar tiempos de respuesta aceptables.
  - Deberán construir el software y/o sistema de información de tal manera que efectúe las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
  - Deberán asegurar que el software y/o sistema de información construido valide la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
  - Deberán suministrar opciones de desconexión o cierre de sesión de los sistemas de información (logout) que permitan terminar completamente con la sesión o conexión asociada, pudiendo ser un cierre de la aplicación, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
  - Deberán asegurar que los sistemas de información proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
  - Deberán garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
  - Deberán remover todas las funcionalidades y archivos que no sean necesarios para el software y/o sistema de información, previo a la puesta en producción.
  - Deberán prevenir la revelación de la estructura de directorios del software y/o sistema de información construido.
  - Deberán remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
  - Deberán evitar incluir las cadenas de conexión a las bases de datos en el código del software y/o sistema de información. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
  - Deberán certificar el cierre de la conexión a las bases de datos desde el software y/o sistema de información tan pronto como estas no sean requeridas.
  - Deberán desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos.
  - Deberán proteger el código fuente de los sistemas de información construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

- Deberán asegurar que no se permite que los sistemas de información desarrollados ejecuten comandos directamente en el sistema operativo.

Elaborado por:	Revisado por:	Homologado por:	Aprobado por:
Julius K. Villavicencio Monti – **Oficial de Seguridad de la Información**	Jorge Herbozo – **Líder de Gobierno Digital**	**Departamento de Planeamiento y Control de Gestión**	Juan Carlos Febres Teves - **Gerente General**
Firma: Firmado digitalmente por: VILLAVICENCIO MONTI Julius Korol FAU 20425809882 hard Fecha: 09/06/2021 16:30:35	**Firma:** Firmado digitalmente por: HERBOZO PEREZ COSTA Jorge Luis Pelayo FAU 20425809882 hard Fecha: 09/06/2021 11:50:42	**NO APLICA**	**Firma:** Firmado digitalmente por: FEBRES TEVES Juan Carlos FAU 20425809882 hard Fecha: 09/06/2021 19:00:59