Política de Desarrollo Seguro de Software

Forestal Collicura Limitada

1. Introducción

La adopción de buenas prácticas de desarrollo de software es fundamental para todas las etapas de desarrollo de un sistema o aplicación de informática, permitiendo un uso correcto e íntegro de estos sistemas, ayudando al usuario final a tener un recurso eficiente, confiable, seguro y privado.

Esta política entrega los lineamientos generales y recomendaciones específicas que debe seguir el área de desarrollo de software al interior de **FORESTAL COLLICURA LIMITADA**, contribuyendo a la construcción de sistemas de alta calidad y seguridad.

2. Objetivo

Definir las directrices generales de seguridad de la información para el desarrollo, adquisición o mantención de los sistemas de información, conforme al ciclo de vida de desarrollo de software y al marco metodológico de **FORESTAL COLLICURA LIMITADA**.

3. Alcance

Los lineamientos y recomendaciones definidas en esta política, deben ser considerados por el área de desarrollo de **FORESTAL COLLICURA LIMITADA** y se aplican a todos los sistemas de información desarrollados internamente y a los que son adquiridos de manera externa, los cuales deberán tener los mismos lineamientos de consideración en relación a la calidad y soporte de seguridad que digan relación con estos aplicativos.

Así también las empresas contratistas que aporten o vendan estos softwares, deberán tener evidencia cierta que estos aplicativos cumplen con todos los estándares, adjuntando los Assesment relacionados y los informes de proveedores especializados en estas materias.

4. Definiciones

Sistema de información: Corresponde a todos los sistemas operativos, infraestructura, aplicaciones y servicios de **FORESTAL COLLICURA LIMITADA**, que permiten administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos de **FORESTAL COLLICURA LIMITADA**.

Entornos o ambientes: Infraestructura tecnológica disponible para alojar y soportar el funcionamiento de sistemas de información, para efectos de su desarrollo, pruebas y operación.

WAF: Web application firewall. Un firewall de aplicaciones web es un tipo de firewall que supervisa, filtra o bloquea el tráfico HTTP hacia y desde una aplicación web.

5. Política

5.1 Lineamientos generales

- Los requisitos de seguridad de la información deben realizarse en la etapa de análisis o levantamiento de requisitos, es decir, previo a la fase de desarrollo, y deben considerar valoraciones de impacto en **FORESTAL COLLICURA LIMITADA** ante posibles fallas de seguridad.

- Los requisitos de seguridad deben ser evaluados como una funcionalidad más del software, debiendo para ello implementar un plan de pruebas documentado permitiendo que el software sea resiliente en relación a sus actualizaciones de seguridad

- Los entornos de desarrollo, pruebas y producción deben permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno productivo.

- El software adquirido desde fuera de la compañía debe contar con soporte del desarrollador o estar debidamente securitizado en función de las recomendaciones de seguridad de la industria, framework o leyes disponibles.

- Considerar el uso de un firewall de aplicación web (WAF) que inspeccione todo el tráfico que fluye a las aplicaciones para ataques comunes de aplicaciones web.

- Considerar para todo efecto el monitoreo en tiempo real de un SOC que analice por medio de estrategias de Ciberinteligencia las conexiones hacia los softwares que sean considerados como críticos, ya sea porque soporten procesos vitales para **FORESTAL COLLICURA LIMITADA**, como por otros que pudieran ser de alto riesgo porque pudieran exponer datos personales de clientes.

- Para efecto de cumplir con los Framework de seguridad de la ISO 27001 y NIST se debe evaluar por medio de un Assesment de seguridad dos veces al año a todo Software ya sea desarrollado internamente como otros que se deban adquirir. Este Assesment no lo deben realizar las mismas casas o vendor que desarrollaron los Softwares.

5.2 Buenas prácticas de desarrollo seguro

5.2.1 Frameworks y librerías de terceros

- Deben utilizarse únicamente componentes de terceros actualizados y de confianza para el software desarrollado por la compañía.
- La validación de estas librerías debe ser por un estamento técnico externo a **FORESTAL COLLICURA LIMITADA.**
- La utilización de estas librerías debe ser detallada completamente en la documentación del Software

5.2.2 Validación de datos

- En todos los campos de entrada de información debe existir una validación para asegurar que sólo los datos con el formato correcto podrán ingresar al sistema.
- La validación de datos debe considerar mecanismos de lista negra (datos conocidos como maliciosos). Y datos de lista blanca (conocidos como correctos) proporcionados por el mismo sistema, por ejemplo a través de listas desplegables.
- Todos los módulos deben tener ambientes de mantención objeto no exista intervención en las base de datos una vez los sistemas estén en productivo.
- La validación de datos debe ser siempre realizada por el lado del servidor. No confundir con avisos al usuario (por ejemplo, para alertar de un campo mal ingresado).

5.2.3 Contraseñas

- Las aplicaciones deben exigir al usuario el uso de contraseñas de características y calidad adecuadas. (Largo 14 caracteres y con complejidad)
- Todos los aplicativos deben usar un mecanismo de doble autentificación objeto bajar la superficie de ataque.
- Una contraseña fuerte es aquélla que es difícil de detectar, tanto por humanos como por software, protegiendo efectivamente los datos de un acceso no autorizado.
- Una contraseña segura consta de al menos catorce (y mientras más caracteres, más fuerte es la contraseña), que son una combinación de letras, números, símbolos y el uso de mayúsculas y minúsculas.
- Para almacenar las contraseñas, se deben utilizar algoritmos criptográficos especialmente diseñados para este fin, tales como bcrypt, PBKDF2 y Argon2. Evitando utilizar algoritmos de hash tradicionales como SHA-1, SHA-2 y MD5 para el almacenamiento de contraseñas.
- Todos los sistemas deben tener la posibilidad de cambiar la contraseña a requerimiento o bajo un calendario administrado.
- Todos los algoritmos criptográficos no pueden estar nombrados o rotulados dentro del código de programación.

5.2.4 Manejo de sesión

Para el manejo de las sesiones se debe considerar como mínimo lo siguiente:

- El identificador de sesión debe ser único, suficientemente largo y aleatorio.
- Se debe implementar un timeout por inactividad que fuerce la Re autenticación al usuario. La duración del timeout debe ser inversamente proporcional a la sensibilidad de los datos a proteger, vale decir, mientras más sensibles, menor duración.

5.2.5 Datos en tránsito

- Las comunicaciones de los componentes que transporten información de los usuarios entre sistemas deberán siempre estar protegidas mediante TLS 1.2 o superior, y los sistemas correctamente configurados para seleccionar el cifrado más fuerte disponible.
- La data en tránsito debe cumplir con todos los estándares de seguridad actual y futura

5.2.6 Calidad del código

- El código debe ser revisado de forma continua durante su construcción con herramientas de análisis estático y dinámico.
- La validación del código antes de producción debe ser realizada bajo un esquema de seguridad total impidiendo la puesta en servicio de sistemas con hallazgos críticos, altos y medio.

5.2.7 Documentación

- Debe existir un repositorio con acceso restringido para la documentación de cada uno de los sistemas desarrollados. Con documentación de las funcionalidades de alto y bajo nivel.

6. Responsabilidades

Área Desarrollo: Encargada del desarrollo y mantención de los sistemas de información de **FORESTAL COLLICURA LIMITADA**, y responsables por adherirse a esta política y seguir los lineamientos y buenas prácticas de desarrollo seguro de software.

Área de ciberseguridad: Encargada de definir los lineamientos de seguridad de la información y de actualizar y velar por el cumplimiento de esta política.

7. Documentación de referencia

El presente documento constituye una política específica destinada al desarrollo seguro de software que sigue los lineamientos del "Framework de Ciberseguridad CIS Controls Versión 8".
Para consultar información más específica y guías de desarrollo seguro de software consultar el: "Estándar de verificación de seguridad en aplicaciones" https://owasp.org/www-pdf-archive/Est%C3%A1ndar_de_Verificaci%C3%B3n_de_Seguridad_en_Aplicaciones_3.0.1.pdf