Política de Gestión de Vulnerabilidades

Forestal Collicura Limitada

Información del Documento

Versión	Fecha de Creación		Descripción
1.0	28-07-2023		Creación y primera versión del documento.

(*) La última versión sustituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los efectos.

Tabla de Contenido

1. Introducción

Con el objetivo de defender y proteger los activos de información y la red de**FORESTAL COLLICURA LIMITADA**, se debe operar en un flujo constante de información, monitorización de los activos, actualizaciones de software, parches, avisos de seguridad, boletines de amenazas, etc.

Comprender y gestionar las vulnerabilidades debe convertirse en una actividad continua, que requiere tiempo, atención y recursos significativos especialmente de las áreas que controlan activos sensibles para **FORESTAL COLLICURA LIMITADA**. Así también si **FORESTAL COLLICURA LIMITADA** no tiene estas capacidades es obligatorio contratar el servicio externo Saas que potencie esta actividad y les permita identificar las vulnerabilidades de sus diferentes activos digitales y físicos de información.

2. Objetivo

Establecer los lineamientos base para el proceso de gestión de vulnerabilidades técnicas, con el propósito de mantener un nivel de aseguramiento adecuado de las plataformas y mitigar los riesgos asociados, adelantándose a explotación de ataques de día Zero, u otros que comprometan los activos de **FORESTAL COLLICURA LIMITADA**.

3. Alcance

Todos los sistemas de información y equipos computacionales que forman parte de la red de la infraestructura (servidores, softwares, equipos de usuarios, redes de telecomunicaciones etc.) y los usuarios responsables por estos activos.

4. Definiciones

Vulnerabilidad: Es una debilidad o deficiencia de seguridad, que puede ser explotada por una amenaza.

Remediación: Acción que permite minimizar el impacto de las vulnerabilidades en **FORESTAL COLLICURA LIMITADA.**

Plan de Remediación: Permite identificar los riesgos asociados a cada vulnerabilidad reportada así como definir los controles que deben ser implementados para mitigar dichos riesgos.

Ethical Hacking: Sirve para explotar las vulnerabilidades existentes en el sistema que se requiere evaluar, valiéndose de un test de intrusión, que permite verificar y evaluar la seguridad física y lógica de sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, entre otros componentes de la infraestructura tecnológica, con la intención de ganar acceso y demostrar que un sistema es vulnerable.

5. Política

5.1 Consideraciones generales

- Todos los servidores o aplicativos de **FORESTAL COLLICURA LIMITADA** deben estar habilitados en una plataforma de monitoreo, la cual permite una detección de vulnerabilidades y gestión de servicios de estos, verificar el estado de sus actualizaciones y otros eventos de significancia para la gestión de las vulnerabilidades.

- Todos los servicios actuales en producción deben tener un test de Vulnerabilidades trimestral activo y es responsabilidad del dueño del activo solicitar este Test y que exista la evidencia de su ejecución por parte del área de ciberseguidad.

- Previa la puesta en producción de cualquier aplicativo o sistema de información se debe realizar un análisis de vulnerabilidades técnicas en un ambiente apropiado para ello. Posteriormente se debe establecer un plan de remediación y seguimiento de las vulnerabilidades identificadas. De acuerdo al riesgo expuesto por la vulnerabilidad, el responsable del activo de información gestionará la remediación y aceptará o no la puesta en producción.

- El análisis de vulnerabilidades técnicas para los sistemas de información y equipos informáticos, debe realizarse periódicamente en base al alcance que determine el área de Ciberseguridad y cada vez que se produzcan cambios significativos en los sistemas de información y equipos informáticos de **FORESTAL COLLICURA LIMITADA**.

- El escaneo de vulnerabilidades que puede afectar a la disponibilidad de los sistemas debe ejecutarse fuera del horario laboral o en periodos de baja carga, y previamente coordinado con los responsables de los sistemas.

- Se considerarán como prioridad del plan de remediación, las vulnerabilidades catalogadas como críticas y altas en base a las metodologías propias de las herramientas de apoyo, para el proceso de escaneo de vulnerabilidades.

- El plan de remediación debe revisarse entre el responsable del activo de información y el especialista de ciberseguridad.

- Si existe un parche disponible de una fuente legítima, deben evaluarse los riesgos asociados con la instalación de este.

- Los parches deben ser probados y evaluados en un entorno controlado antes de su instalación masiva, con el fin de garantizar que son efectivos y que no tienen efectos secundarios que no puedan ser aceptados.

- Si no hay ningún parche disponible, deberían considerarse otros controles, como:

- La desactivación de servicios o capacidades relacionadas con la vulnerabilidad.
- El incremento de la supervisión para detectar o evitar ataques reales.
- El aumento de la concienciación sobre la vulnerabilidad

- Una vez ejecutado el plan de remediación, se debe realizar un segundo análisis de vulnerabilidades (retest), para verificar si la implementación fue satisfactoria. El sistema no podrá ser puesto en producción si se mantienen las vulnerabilidades.
- Ningún sistema que se exponga hacia servicios públicos podrá ser puesto en producción sin la autorización del área de Ciberseguridad.
- Los sistemas internos y que no se expongan hacia Internet de igual forma deberán tener validaciones por parte del área de Ciberseguridad.
- Si un sistema o servicio, por condiciones técnicas insalvables debiera convivir con vulnerabilidades, se analizarán los controles mitigadores que pudieran bajar el riesgo objetivo hacer viable su funcionamiento y será el cargo más alto de **FORESTAL COLLICURA LIMITADA** quien debiera autorizar esta puesta en servicio.

6. Responsabilidades

Área de Ciberseguridad: Es el responsable de definir el alcance para realizar el procedimiento para la gestión de vulnerabilidades técnicas, sobre los sistemas de información y equipos informáticos de **FORESTAL COLLICURA LIMITADA** y conocer los resultados de dicho análisis y pedir la gestión de esas vulnerabilidades por parte de las áreas dueñas de los activos.

Responsable del activo de información: Responsable de ejecutar las acciones de remediación que se efectuarán, asumiendo los riesgos de aquellas que no se puedan

ejecutar y elaborando el plan de remediación, previa coordinación con el Jefe de Ciberseguridad.

Especialista de Ciberseguridad: Responsable de la ejecución del escaneo de vulnerabilidades y seguimiento de los planes de remediación.

Jefe de SOC/proveedor externo SOC: Debe estar en conocimiento de las diversas plataformas de **FORESTAL COLLICURA LIMITADA** y junto a su equipo debe monitorear las gestiones de las distintas vulnerabilidades, informando al área de Ciberseguridad los cambios o registros importantes de las plataformas.

7. Documentación de referencia

El presente documento constituye una política específica destinada a la gestión de vulnerabilidades técnicas que sigue los lineamientos del Código de prácticas para los controles de seguridad de la información ISO/IEC 27002". De esta política se desprenderán los procedimientos específicos relacionados con los temas de Gestión de Vulnerabilidades de cada área.