INFORME DE CIBERSEGURIDAD
INSTITUTO DE CULTURA Y TURISMO DE BOLIVAR - ICULTUR

Introducción:
El presente informe tiene como objetivo analizar las vulnerabilidades en la infraestructura de tecnologías de la información del ICULTUR, así como proponer soluciones y acciones para mejorar la seguridad cibernética de la organización. Se identificarán los hallazgos encontrados y se presentarán recomendaciones para mitigar los riesgos actuales y futuros.

Objetivo General:

Fortalecer la postura de ciberseguridad del Instituto de Cultura y Turismo de Bolívar (ICULTUR) mediante la implementación de medidas y políticas que mitiguen las vulnerabilidades existentes y promuevan la protección de los activos de información, garantizando así la continuidad de las operaciones y el cumplimiento de las normativas legales.

Objetivos Específicos:

- **Regularización de Licenciamiento de Software:**
    - Identificar y adquirir las licencias faltantes de software para todos los equipos y sistemas utilizados por el ICULTUR.
    - Establecer un proceso de gestión de licencias para mantener la conformidad continua y evitar sanciones legales.
- **Implementación de Servidor de Dominio de Red:**
    - Adquirir e implementar un servidor de dominio de red para centralizar la gestión de usuarios y recursos.
    - Configurar políticas de acceso y seguridad para proteger los activos de información y restringir el acceso no autorizado.
- **Mejora de Políticas de Seguridad Informática:**

- Adquirir e implementar un sistema antivirus licenciado para todos los equipos del ICULTUR.
- Revisar y actualizar las políticas de seguridad informática para abordar vulnerabilidades y mitigar riesgos.
- Evaluar y considerar la implementación de soluciones adicionales, como sistemas de detección y prevención de intrusos, para fortalecer la seguridad de la red.

Análisis de Vulnerabilidades

Licenciamiento de Software:

La falta de licenciamiento de los sistemas operativos y software de ofimática expone a la entidad a sanciones legales y decomisos de equipos. Es imperativo regularizar las licencias para cumplir con las normativas legales y evitar riesgos legales y de seguridad.

- **Acción a tomar:** Realizar un inventario de software, adquirir licencias faltantes y establecer un proceso de gestión de licencias para mantener la conformidad continua.

Seguridad Informática:

Aunque se cuenta con un equipo básico de seguridad (Firewall Meraky), la falta de un sistema antivirus licenciado deja expuestos algunos equipos a amenazas de malware. Además, la implementación de un nuevo equipo de control de borde es un paso positivo, pero se requiere una estrategia integral de seguridad.

- **Acción a tomar:** Adquisición e implementación de un sistema antivirus licenciado para todos los equipos, revisión y mejora de políticas de seguridad, y evaluación de soluciones de seguridad adicionales como sistemas de detección y prevención de intrusos.

A continuación, se describe una propuesta de mejora para reforzar las debilidades que se presentan en ciber seguridad de ICULTUR:

Propuesta de servicios de seguridad informática: Implementación de Soluciones de Firewall, Switching y WiFi con Fortinet:

- ✓ Adquirir e implementar dispositivos de firewall, switching y puntos de acceso WiFi de Fortinet para fortalecer la seguridad de la red del ICULTUR.
- ✓ Configurar políticas de seguridad avanzadas en el firewall para proteger la red interna de amenazas cibernéticas y controlar el tráfico de red.
- ✓ Implementar funciones de switching avanzadas para optimizar el rendimiento de la red y garantizar una conectividad confiable y segura entre los diferentes dispositivos y segmentos de la red.

- ✓ Desplegar puntos de acceso WiFi de Fortinet para mejorar la cobertura y el rendimiento del sistema WiFi, garantizando una conexión estable y segura para los usuarios del I.

Solución Propuesta:

Para abordar las necesidades de seguridad de red de CULTUR, se propone la implementación de soluciones de firewall, switching y WiFi de Fortinet. Fortinet es un proveedor líder en seguridad de red que ofrece una amplia gama de productos y servicios diseñados para proteger las redes de las organizaciones contra amenazas cibernéticas.

Firewall FortiGate:

Adquisición e implementación de dispositivos de firewall FortiGate para proteger la red del ICULTUR contra amenazas cibernéticas. Los dispositivos FortiGate ofrecen funciones de firewall de última generación (NGFW) que incluyen inspección profunda de paquetes, filtrado de contenido, prevención de intrusiones y detección de amenazas avanzadas. Configuración de políticas de seguridad personalizadas en el firewall FortiGate para controlar el tráfico de red, restringir el acceso no autorizado a recursos sensibles y prevenir ataques cibernéticos.

Switches FortiSwitch:

Implementación de switches FortiSwitch para proporcionar conectividad de red confiable y segura en las instalaciones de ICULTUR. Los switches FortiSwitch ofrecen funciones avanzadas de switching, como virtual LAN (VLAN), calidad de servicio (QoS) y seguridad de puertos para optimizar el rendimiento de la red y garantizar una comunicación fluida entre los dispositivos. Configuración de políticas de seguridad en los switches FortiSwitch para segmentar la red y limitar el acceso a recursos específicos según las necesidades de la organización.

Puntos de Acceso WiFi FortiAP:

Despliegue de puntos de acceso WiFi FortiAP para mejorar la cobertura y el rendimiento del sistema WiFi de ICULTUR. Los puntos de acceso FortiAP ofrecen conectividad inalámbrica segura y confiable para usuarios y dispositivos, garantizando una experiencia de usuario óptima. Configuración de políticas de seguridad en los puntos de acceso FortiAP para proteger la red inalámbrica contra intrusiones y ataques cibernéticos, así como para proporcionar acceso seguro a los usuarios autorizados.

Plan de Mejoras:

- Regularización de Licenciamiento de Software.
- Implementación de Servidor de Dominio de Red.
- Mejora de Políticas de Seguridad Informática.
- Actualización y Mejora de Infraestructura de Red.

- Se recomienda que la próxima administración de ICULTUR priorice la implementación de estas medidas para fortalecer la seguridad cibernética y garantizar el funcionamiento óptimo de la infraestructura de tecnologías de la información.

Este informe pretende servir como guía para la toma de decisiones y la asignación de recursos en materia de ciberseguridad en ICULTUR. Se recomienda realizar evaluaciones periódicas y ajustes según las necesidades y evolución de las amenazas cibernéticas.
Acciones Recomendadas:

Regularización de Licenciamiento de Software:

- Realizar un inventario detallado del software utilizado en la organización.
- Adquirir licencias faltantes para garantizar el cumplimiento legal.
- Implementar un proceso de gestión de licencias para mantener la conformidad continua.

Implementación de Servidor de Dominio de Red:

- Adquirir e implementar un servidor de dominio de red para centralizar la gestión de usuarios y recursos.
- Configurar políticas de acceso y seguridad para proteger los activos de información.

Mejora de Políticas de Seguridad Informática:

- Adquisición e implementación de un sistema antivirus licenciado para todos los equipos.
- Revisión y mejora de las políticas de seguridad para abordar vulnerabilidades y mitigar riesgos.
- Evaluación de soluciones adicionales como sistemas de detección y prevención de intrusos para una defensa en capas.

Actualización y Mejora de Infraestructura de Red:

- Realizar una evaluación completa de la infraestructura de red para identificar deficiencias.
- Corregir problemas de cableado estructurado para mejorar la transmisión de datos.
- Mejorar la cobertura y el rendimiento del sistema WiFi para proporcionar una experiencia de usuario óptima.
- Implementar segmentación de red adecuada para aislar áreas sensibles y proteger la privacidad de la información.
- Considerar la autogestión de equipos de red para una administración eficiente y oportuna.

Se espera que la implementación de estas acciones mejore significativamente la postura de ciberseguridad de ICULTUR, reduciendo la exposición a amenazas cibernéticas, garantizando el cumplimiento legal y mejorando la eficiencia operativa de la organización. Además, estas medidas

proporcionarán una base sólida para adaptarse a las necesidades cambiantes del entorno cibernético y proteger los activos de información críticos del instituto.