Ciencia, Tecnología e Innovación
Gobierno de la República

HONDURAS
GOBIERNO DE LA REPÚBLICA

senacit

Disposiciones de uso obligatorio para prevenir e idenficar oportunamente riesgos a la seguridad de los sistemas operativos, las redes, aplicaciones y otros recursos tecnologicos.

Tegucigalpa, Honduras, Tel. +504 22311898

SENACIT@gob_Honduras

Introducción

En la era digital actual, la seguridad de los sistemas operativos, redes, aplicaciones y otros recursos tecnológicos se ha convertido en una prioridad crítica para organizaciones de todos los tamaños y sectores. La creciente dependencia de la tecnología para la realización de operaciones diarias, la gestión de datos sensibles y la comunicación interna y externa ha aumentado exponencialmente el riesgo de ciberataques y brechas de seguridad. Por ello, es fundamental implementar un conjunto robusto de disposiciones de uso obligatorio para prevenir e identificar oportunamente estos riesgos.

Estas disposiciones abarcan una amplia gama de políticas, controles técnicos y prácticas operativas diseñadas para proteger los activos tecnológicos de amenazas tanto internas como externas. Las políticas de seguridad establecen las directrices y estándares que todos los empleados de la Institución **SENACIT/IHCIETI** deben seguir para garantizar un entorno seguro. Los controles técnicos, como antivirus, firewalls y sistemas de detección de intrusos, proporcionan barreras efectivas contra accesos no autorizados y software malicioso. Además, las prácticas operativas, incluyendo el monitoreo continuo y las auditorías de seguridad, aseguran la vigilancia constante y la mejora continua de las defensas de seguridad.

1. Políticas de Seguridad

- **Política de Contraseñas**: Establecer requisitos de complejidad, longitud y caducidad de las contraseñas.
- **Política de Acceso**: Definir quién tiene acceso a qué recursos y bajo qué condiciones. Implementar el principio de menor privilegio.
- **Política de Actualización**: Asegurar que todos los sistemas y aplicaciones estén actualizados con los últimos parches de seguridad.
- **Política de Uso Aceptable**: Establecer normas claras sobre el uso adecuado de los recursos tecnológicos.

2. Controles Técnicos

- **Antivirus y Antimalware**: Implementar y actualizar regularmente software de protección contra virus y malware.
- **Firewalls**: Configurar firewalls para proteger redes internas de accesos no autorizados.
- **Sistemas de Detección y Prevención de Intrusos (IDS/IPS)**: Monitorear y bloquear actividades sospechosas o no autorizadas.
- **Cifrado**: Utilizar cifrado para proteger datos sensibles tanto en tránsito como en reposo.

3. Prácticas Operativas

- **Monitoreo Continuo**: Implementar sistemas de monitoreo continuo para detectar y responder rápidamente a incidentes de seguridad.
- **Auditorías de Seguridad**: Realizar auditorías periódicas para evaluar la efectividad de las medidas de seguridad implementadas.
- **Copia de Seguridad (Backups)**: Realizar copias de seguridad regulares y asegurar que los backups se almacenen de manera segura.
- **Pruebas de Penetración**: Llevar a cabo pruebas de penetración periódicas para identificar y mitigar vulnerabilidades.

4. Capacitación y Concientización

- **Entrenamiento Regular**: Capacitar a los empleados sobre las mejores prácticas de seguridad y cómo identificar amenazas comunes, como phishing.
- **Simulacros de Incidentes**: Realizar simulacros de incidentes de seguridad para preparar al personal para responder adecuadamente.

5. Gestión de Vulnerabilidades

- **Evaluación de Vulnerabilidades**: Realizar evaluaciones regulares de vulnerabilidades en los sistemas y aplicaciones.
- **Gestión de Parches**: Implementar un proceso sistemático para la aplicación de parches y actualizaciones.

6. Respuesta a Incidentes

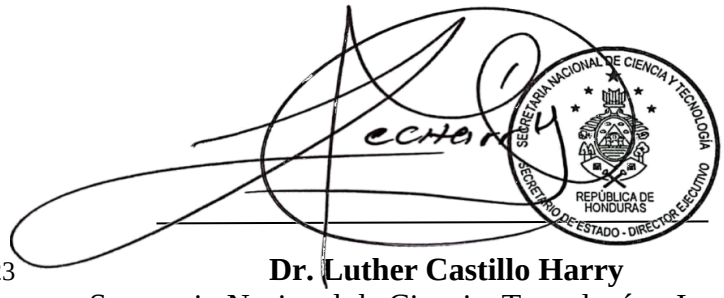
- **Plan de Respuesta a Incidentes**: Desarrollar y mantener un plan de respuesta a incidentes que detalle los procedimientos a seguir en caso de un incidente de seguridad.
- **Equipo de Respuesta a Incidentes**: Formar un equipo dedicado a la respuesta rápida y eficaz a incidentes de seguridad.

7. Control de Acceso Físico

- **Seguridad Física**: Implementar medidas de seguridad física para proteger los recursos tecnológicos contra accesos no autorizados.

8. Protección de Datos

- **Clasificación de Datos**: Establecer un sistema de clasificación de datos para identificar y proteger adecuadamente la información sensible.
- **Política de Retención de Datos**: Definir cuánto tiempo se debe conservar la información y cómo debe ser eliminada de manera segura.



Aprobado por:
Fecha: 12/8/2023

Dr. Luther Castillo Harry
Secretario Nacional de Ciencia, Tecnología e Innovación