Política de seguridad de la información: Resumen

Identificación del documento

Código: PR00-MGSI-POLITICA-WEB

Revisiones:

Revisión	Fecha	Descripción
1.0	2024-01-16	Versión resumida de la política general
1.1	2024-01-25	Nueva redacción de ámbito

Objetivo

La política de seguridad de la información de IPROCURATIO busca preservar la confidencialidad, integridad y disponibilidad de la información. Su objetivo es establecer requisitos para proteger la información y los servicios tecnológicos de la organización. Se basa en principios como alcance estratégico, seguridad integral, gestión de riesgos, proporcionalidad, mejora continua y seguridad por defecto.

La dirección de IPROCURATIO se compromete a promover funciones y responsabilidades en seguridad de la información, proporcionar recursos adecuados, divulgar y concienciar sobre la política, exigir su cumplimiento y considerar los riesgos en la toma de decisiones.

Se establecen roles y responsabilidades, donde el responsable de la información tiene un mandato de dos años. También se destaca la importancia de la formación y concienciación del personal en seguridad de la información.

La política aborda la gestión de activos, dispositivos BYOD (Bring Your Own Device), el ciclo de vida de la información y la gestión de copias de seguridad. Se establece la necesidad de realizar pruebas de restauración periódicas y se promueve la ubicación segura de copias de respaldo.

Se implementa una clasificación de la información basada en niveles de sensibilidad, considerando soportes lógicos y físicos. Además, se abordan requisitos específicos para dispositivos BYOD, mesas limpias, gestión de activos y ciclo de vida de la información.

Ámbito de Aplicación en Desarrollo de Aplicaciones Sanitarias

En el marco de la Política de Seguridad de la Información de IPROCURATIO, el ámbito de aplicación es el relacionado con el desarrollo de aplicaciones sanitarias y aborda consideraciones críticas para garantizar la confidencialidad, integridad y disponibilidad de la información en este contexto específico.

Específicamente, el ámbito de aplicación es:

> EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN QUE DA SOPORTE AL DESARROLLO A MEDIDA DE SISTEMAS PARA TERCEROS DE PRODUCTOS EN EL CAMPO DE SALUD SEGÚN LA DECLARACIÓN DE APLICABILIDAD V1.0

Política de Seguridad de la Información

1. **Manipulación de la Información:**
    - Desarrollo e implementación de procedimientos para la correcta manipulación de la información.
    - Custodia continua de la información privilegiada durante todo su ciclo de vida.
2. **Privacidad de la Información:**
    - Asegurar la privacidad de los datos de carácter personal.
    - Cumplimiento de la legislación vigente en materia de protección de datos personales.
    - Implementación de medidas para garantizar la privacidad de la información en todas las fases de su ciclo de vida.
3. **Prevención de Fugas de Información:**
    - Análisis de los vectores de fuga de información.
    - Identificación de activos con mayor riesgo de fuga.
    - Definición de procedimientos para prevenir la pérdida de información.
    - Formación y capacitación de socios en buenas prácticas para la prevención de fugas de información.
4. **Control de Acceso:**
    - Implementación de un sistema de control de acceso en todos los sistemas de información.
    - Requisitos de negocio para el control de acceso, como la unicidad de usuarios y la prohibición de usuarios genéricos.
    - Definición de derechos de acceso basados en roles y principios de mínimo privilegio.
5. **Gestión del Ciclo de Vida de la Identidad:**
    - Definición e implementación de un sistema de gestión del ciclo de vida de la identidad.
    - Actividades que abarcan la creación, revisión periódica, modificación y eliminación de identidades.
6. **Seguridad Física y del Entorno:**
    - Protección adecuada de los espacios físicos que albergan sistemas de información.
    - Control de acceso físico a la información en formato físico.
    - Medidas específicas para la seguridad de activos físicos que contienen información reservada o secreta.
7. **Seguridad en el Trabajo en la Nube o Cloud:**

- Mantenimiento de una política de trabajo en la nube con medidas de seguridad para la confidencialidad, integridad y disponibilidad de la información.

8. **Seguridad Operativa:**
    - Implementación de medidas de seguridad en sistemas que procesan o almacenan información.
    - Gestión, control y monitorización adecuados de las redes.
9. **Seguridad en las Telecomunicaciones:**
    - Administración de seguridad en las redes internas y externas.
    - Establecimiento de pautas de seguridad para la transferencia de información y el uso de dispositivos y servicios.
10. **Seguridad en el Ciclo de Vida del Desarrollo de Sistemas:**
    - Requisitos mínimos de seguridad en la adquisición, desarrollo y mantenimiento de sistemas y datos.
    - Gestión de pruebas, seguimiento de cambios e inventario de software.
11. **Seguridad en los Proveedores:**
    - Evaluación de la criticidad de servicios susceptibles de ser subcontratados.
    - Consideración de medidas contractuales y de seguridad al seleccionar y evaluar proveedores.
12. **Gestión de Incidentes:**
    - Obligación de notificar cualquier incidente que pueda comprometer la seguridad de los activos de información.
    - Implementación de procedimientos para la gestión de incidentes.
13. **Continuidad de Negocio:**
    - Desarrollo de un Plan de Continuidad de Negocio para garantizar la continuidad en la prestación de servicios esenciales.
    - Formación y capacitación en Continuidad de Negocio para todos los socios.
14. **Cumplimiento Regulatorio:**
    - Compromiso con el cumplimiento de toda legislación, normativa o regulación aplicable.
15. **Auditorías de Seguridad y Gestión de Vulnerabilidades:**
    - Identificación periódica de vulnerabilidades y aplicación de medidas correctoras basadas en riesgos.
16. **Gestión del Cambio:**
    - Registro e informe de cualquier cambio en la política de seguridad.
    - Análisis de riesgos asociados a cambios y asunción de riesgos por parte del solicitante y responsables del negocio.
17. **Sanciones Disciplinarias:**

- Adopción de acciones disciplinarias en caso de violación de la política de seguridad.

18. **Revisión de la Política:**
    - Revisión y aprobación anual por el Consejo de Administración.
    - Revisiones adicionales en caso de cambios relevantes en la sociedad o en el entorno de amenazas.

Esta política integral aborda diversos aspectos cruciales para garantizar la seguridad de la información y la continuidad de negocio en IPROCURATIO.

Aspectos CID (Confidencialidad, Integridad y Disponibilidad)

En la política de seguridad de la información para IPROCURATIO, los aspectos de CID (Confidencialidad, Integridad y Disponibilidad) son fundamentales para garantizar la protección y gestión efectiva de la información. A continuación, se resumen cómo se abordan estos aspectos en diferentes secciones de la política:

1. **Confidencialidad:**
    - **Control de Acceso (Sección 11):** Se implementa un sistema de control de acceso en todos los sistemas de información. Esto garantiza que solo las personas autorizadas tengan acceso a la información, preservando su confidencialidad.
    - **Privacidad de la Información (Sección 9):** Se asegura la privacidad de los datos de carácter personal, cumpliendo con la legislación de protección de datos. Esto contribuye a mantener la confidencialidad de la información sensible.

2. **Integridad:**
    - **Control de Acceso (Sección 11):** La definición de derechos de acceso basados en roles y principios de mínimo privilegio contribuye a preservar la integridad de la información al evitar modificaciones no autorizadas.
    - **Seguridad en el Ciclo de Vida del Desarrollo de Sistemas (Sección 17):** Se establecen requisitos mínimos de seguridad en el desarrollo y mantenimiento de sistemas, asegurando la integridad de los datos durante todo su ciclo de vida.

3. **Disponibilidad:**
    - **Continuidad de Negocio (Sección 20):** La elaboración de un Plan de Continuidad de Negocio garantiza la disponibilidad de servicios esenciales incluso en situaciones de crisis o interrupciones.
    - **Seguridad Operativa (Sección 15):** Se implementan medidas de seguridad en sistemas para asegurar la disponibilidad de la información y se gestiona y controla adecuadamente la infraestructura de red.

4. **Gestión del Ciclo de Vida de la Identidad (Sección 12):**
    - La gestión adecuada del ciclo de vida de la identidad contribuye a la confidencialidad y la integridad, ya que se asegura de que solo personas autorizadas tengan identidades válidas, reduciendo el riesgo de usurpación de identidad.

5. **Prevención de Fugas de Información (Sección 10):**
    - Al analizar los vectores de fuga de información y establecer procedimientos para prevenir la pérdida de información, se protege la confidencialidad y la integridad de los datos.
6. **Seguridad en el Trabajo en la Nube o Cloud (Sección 14):**
    - Mantener una política de trabajo en la nube con medidas de seguridad contribuye a preservar la confidencialidad, la integridad y la disponibilidad de la información almacenada en entornos en la nube.
7. **Seguridad en las Telecomunicaciones (Sección 16):**
    - La administración de seguridad en las redes internas y externas asegura la disponibilidad y la integridad de las comunicaciones, evitando interrupciones y manipulaciones no autorizadas.

La política aborda estos aspectos de CID de manera integral para asegurar que la información en IPROCURATIO esté protegida contra amenazas a la confidencialidad, integridad y disponibilidad.