UNIVERSIDAD AUTÓNOMA
DEL ESTADO DE MÉXICO

Facultad de Ingeniería

MATERIA: Seguridad de la información

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Docente:
Alejandro Hernández Arriaga

Alumno:
Ulises Becerril Valdés

Grupo:01

Ciclo escolar 2023B

22 de marzo de 2023

Sumario

TAREA 1: Elementos de una política de seguridad de la información

Una política es una declaración de alto nivel, documentación con base en las creencias, objetivos y metas de la empresa, la cual establece las decisiones de como debe ser manejada y protegida la información que maneja esta organización.

Estas políticas involucran alojamiento de los recursos, estrategias de protección de los recursos técnicos y de la información así como guías de comportamiento de los empleados.

Definiciones

Política: Es una declaración de los objetivos de una empresa y los medios generales para poder alcanzarlos en un área específica, debe ser breve y establecerse en un alto nivel.

Política de propósito general: Establece las condiciones de comportamiento general y asignación de recursos para su propia implementación.

Políticas de tema específico: Aborda cuestiones específicas de interés para la organización, como puede ser el uso del correo electrónico, internet, teléfono móvil, etc.

Política de seguridad de la información: Es una declaración que establece las metas y objetivos además de los medios generales para poder lograr un manejo y seguridad adecuado de la información dentro de la organización. Una política de seguridad de la información nunca establece como es que se deben lograr estos objetivos, es por esta razón por lo que las organizaciones deben desarrollar normativas, derectrices y procedimientos para poder implementar estas políticas y conseguir sus objetivos.

Elementos de una política de seguridad de la información

- **Propósito**

Breve descripción de la política, a quien está dirigida, explicación de por que es necesaria incluidos los objetivos de seguridad de la información así como los que la organización desea alcanzar.1

- **Alcance**

Define a quien aplica la política (empleados, gerentes, gefes de área, etc) y los recursos de la información que abarca.

- **Definiciones y términos**

Definiciones el términos técnicos de seguridad para asegurar que todos los lectores tengan la comprensión común del texto en general.

- **Principios**

Cumplimiento de las leyes y regulaciones, exposición mínima y máxima de la información y gestión de riesgos.

- **Roles y responsabilidades**

Descripción de los roles dentro de la organización y sus responsabilidades al asumir estos roles para la implementación específica de la política.

- **Control de incidentes de seguridad**

Procedimientos para reportar y gestionar los incidentes de seguridad, incluyendo la investigación, registro y resolución de los incidentes.

- **Procedimientos y guías de implementación**

Documentos de apoyo y estipulación en los que se detallan como es que se deben implementar las directrices de la política en la práctica diaria.

- **Sanciones**

Descripción de las consecuencias de no cumplir con la política.

TAREA 2: Ejemplos de políticas de seguridad de la información

1. Política de gestión de contraseñas

Resumen

Esta política establece los requisitos para crear, distribuir y mantener contraseñas seguras para proteger los recursos de información de la organización.

Introducción

Las contraseñas son una de las primeras líneas de defensa en la seguridad de la información. Una gestión adecuada es crucial para proteger los accesos autorizados y prevenir accesos no autorizados.

Alcance

Aplica a todos los empleados, contratistas y terceros que acceden a sistemas internos de la organización.

Objetivos

- Establecer criterios para la creación de contraseñas seguras.
- Definir procedimientos para el cambio regular de contraseñas.
- Asegurar el almacenamiento y transmisión segura de contraseñas.

Responsabilidades

- **Empleados**: Crear contraseñas conforme a los criterios establecidos y cambiarlas regularmente.
- **Departamento de IT**: Proveer sistemas que soporten políticas de contraseñas seguras y realizar auditorías periódicas.
- **Seguridad de la Información**: Establecer los estándares de contraseñas seguras y educar a los usuarios sobre prácticas seguras.

KPIs

- Porcentaje de contraseñas que cumplen con los estándares de complejidad.
- Número de incidentes de seguridad relacionados con contraseñas débiles o comprometidas.
- Frecuencia de cambios de contraseñas en sistemas críticos.

2. Política de respuesta a incidentes

Resumen

Directrices para la detección, reporte y respuesta a incidentes de seguridad de la información, minimizando el impacto y restaurando la operatividad.

Introducción

La gestión eficaz de incidentes de seguridad es vital para la resiliencia operativa y la protección de activos críticos.

Alcance

Cubre a todos los empleados y sistemas de información de la organización.

Objetivos

- Detectar y reportar rápidamente incidentes de seguridad.
- Responder y mitigar el impacto de incidentes de seguridad.
- Registrar y aprender de los incidentes para mejorar la seguridad.

Responsabilidades

- **Todos los Empleados**: Reportar inmediatamente cualquier sospecha de incidente de seguridad.
- **Equipo de Respuesta a Incidentes**: Gestionar la respuesta y recuperación ante incidentes.
- **Seguridad de la Información**: Analizar incidentes para mejorar las políticas y controles de seguridad.

KPIs

- Tiempo medio de detección de incidentes.
- Tiempo medio de respuesta y resolución de incidentes.
- Número de incidentes recurrentes de similar naturaleza.

3. Política de gestión de accesos

Resumen

Establece el marco para garantizar que el acceso a los sistemas y datos es otorgado de acuerdo con los principios de menor privilegio y necesidad de conocer.

Introducción

Un control de acceso efectivo es esencial para proteger la confidencialidad, integridad y disponibilidad de la información.

Alcance

Afecta a todos los sistemas, redes y aplicaciones de la organización, y aplica a empleados, contratistas y terceros.

Objetivos

- Asegurar que los accesos son otorgados de manera adecuada y revisados periódicamente.
- Minimizar el riesgo de accesos no autorizados.
- Facilitar el cumplimiento de normativas y auditorías.

Responsabilidades

- **Gerentes**: Solicitar accesos adecuados para sus equipos y aprobar solicitudes de acceso.
- **Departamento de IT**: Implementar controles de acceso y realizar revisiones de accesos.
- **Departamento de seguridad de la información**: Definir políticas de gestión de accesos y realizar auditorías periódicas.

KPIs

- Número de violaciones de acceso detectadas.
- Tiempo medio para la revocación de accesos una vez que son solicitados.
- Porcentaje de revisiones de acceso completadas en el tiempo definido.

Bibliografía

- Peltier, T. (2001). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. http://ci.nii.ac.jp/ncid/BA60132863