POLITICAS DE SEGURIDAD INFORMÁTICA:

JEAN CARLOS MAYORCA

SANTIAGO RODRIGUES

VICTOR MANUEL PEMBERTY.

**INTRODUCCION**

Las Políticas de Seguridad Informática son un conjunto de directrices y reglas diseñadas para salvaguardar la información y los recursos informáticos de una organización. Su principal objetivo es proteger la confidencialidad, integridad y disponibilidad de los datos frente a amenazas cibernéticas. Estas políticas establecen normas para el acceso, autenticación, gestión de contraseñas, copias de seguridad y muchas otras áreas relacionadas con la seguridad de la información. Son esenciales para garantizar la seguridad digital en un entorno empresarial y cumplir con regulaciones y estándares de seguridad.

1.1Propósito de la política: Él propósito de la política de seguridad informática es como establecer las reglas y normas para proteger nuestras computadoras y datos en línea, evitando que personas no autorizadas entren y causen problemas. También nos ayuda a saber qué hacer en caso de problemas, como contraseñas olvidadas o ataques cibernéticos, y nos dice cómo debemos comportarnos en línea para mantenernos seguros y proteger la información importante. En resumen, es como un conjunto de reglas para mantener nuestra información y nuestras computadoras a salvo.

1.2. Alcance de la política: El alcance de esta política de seguridad informática se enfoca en definir hasta dónde llegan las reglas y normas que debemos seguir. Esto significa que nos dice a qué aspectos de la seguridad informática se aplican estas reglas y a cuáles no. Por ejemplo, nos dice qué computadoras y sistemas están cubiertos por estas reglas y quiénes deben cumplirlas. En otras palabras, establece los límites de las reglas de seguridad informática que debemos seguir.

1.3. Responsabilidades y autoridades: Las responsabilidades y autoridades en esta política de seguridad informática se refieren a las tareas que cada persona debe hacer y el poder que tienen para asegurarse de que todo funcione correctamente y esté seguro en cuanto a la computadora y la información. Esto significa que algunas personas tienen la responsabilidad de mantener las contraseñas seguras y otras de asegurarse de que nadie entre en las computadoras sin permiso. También nos dice quién está a cargo de tomar decisiones importantes sobre la seguridad informática, como qué hacer si algo sale mal. En resumen, establece quién hace qué y quién tiene el poder de tomar decisiones en cuanto a la seguridad informática.

**Categorización de la información**

La categorización de la información se refiere a la clasificación y organización de los datos y la información en diferentes niveles de confidencialidad o importancia. Esto se hace para gestionar adecuadamente la seguridad de la información y determinar quién tiene acceso a qué tipo de datos.

2.1. Clasificación de la información: Clasificar la información significa ordenarla o separarla en grupos según cuán importante o secreta sea. Es como cuando organizas tus juguetes en diferentes cajas: algunos son muy especiales y van en una caja especial, otros son menos importantes y van en otra caja. De esta manera, sabes dónde está cada cosa y quién puede jugar con ellas. La clasificación de la información ayuda a saber qué datos son muy importantes y deben protegerse con mucho cuidado, y cuáles no son tan críticos.

2.2. Propiedad de la información: La propiedad de la información es como decir quién es el dueño de los datos. Piensa en ello como si fueras el dueño de una bicicleta. La bicicleta es tuya, y puedes decidir quién puede usarla y quién no. De manera similar, la propiedad de la información significa que algunas personas son las dueñas de ciertos datos o información. Ellas pueden decidir quién tiene permiso para ver o usar esa información, y quién no. Es importante porque ayuda a proteger la información y asegurarse de que se utilice adecuadamente.

2.3. Etiquetado y manejo de los datos: El etiquetado y manejo de los datos es como poner nombres o etiquetas en tus cosas para saber qué son y cómo debes cuidarlas.

Imagina que tienes una caja de juguetes. Para saber qué hay dentro y cómo debes cuidarlos, pones etiquetas en cada juguete. Algunos pueden tener una etiqueta que dice "frágil", lo que significa que debes ser cuidadoso con ellos. Otros pueden tener una etiqueta que dice "compartir", lo que significa que puedes prestarlos a tus amigos. El etiquetado de datos es algo similar, pero en lugar de juguetes, son archivos o información en una computadora.

Cuando etiquetas y manejas datos, les das un nombre o una descripción para saber qué son y cuán importantes son. También puedes decir quién puede usarlos y cómo deben ser protegidos. Esto ayuda a mantener la información organizada y segura.

**Acceso a la información**: Acceder a la información es como abrir un libro o una carpeta para ver lo que está dentro. Cuando tienes acceso a la información, significa que puedes mirarla o usarla. Es como si te dieran una llave para abrir una puerta y ver lo que hay adentro. Pero, a veces, no todos pueden acceder a la misma información; depende de las reglas o permisos que tengan. Algunas personas pueden acceder a cierta información, mientras que a otras no se les permite. Es como cuando algunos amigos pueden jugar con tus juguetes, pero otros no pueden. El acceso a la información se trata de quién puede ver o usar ciertos datos y quién no.

3.1. Controles de acceso: Los controles de acceso son como reglas o candados que ayudan a decidir quién puede entrar o usar algo importante. Es como si tuvieras una caja de juguetes con una cerradura y solo tú tuvieras la llave. Los controles de acceso son como esa llave; te permiten decidir quién más puede jugar con tus juguetes.

Cuando aplicamos controles de acceso a la información en una computadora, estamos asegurándonos de que solo las personas autorizadas puedan ver o usar esos archivos o programas. Es como tener una lista de invitados para una fiesta: solo las personas en la lista pueden entrar. Los controles de acceso protegen la información importante y evitan que personas no autorizadas la vean o cambien.

3.2. Autenticación y autorización: La autenticación es como demostrar quién eres antes de que te dejen hacer algo importante. Piensa en ello como cuando llegas a casa después de la escuela y la puerta está cerrada. Para entrar, necesitas mostrar a tu mamá o papá que eres tú. Puedes hacerlo diciendo tu nombre o usando una llave especial. Eso es la autenticación: confirmar tu identidad.

3.3. Administración de contraseñas: La administración de contraseñas es como cuidar y organizar las claves secretas que usamos para proteger nuestras cuentas en línea, como si fueran tesoros muy valiosos.

3.4. Gestión de identidad: La gestión de identidad nos ayuda a estar seguros en línea y asegurarnos de que nadie más se haga pasar por nosotros en el mundo digital

**Protección de la información**

4.1. Protección de los activos de información: Describe cómo se protegen los datos.

4.2. Protección contra malware: Establece políticas para protegerse contra el malware.

4.3. Protección contra amenazas internas y externas: Describe cómo se protegen los sistemas contra amenazas.

4.4. Protección de la red y de los sistemas: Define las medidas para proteger la red y los sistemas.

**Seguridad física**

5.1 Medidas de seguridad física: Aunque es un comercio electrónico, aún puede ser necesario proteger el hardware físico.

5.2 Control de acceso físico: Define quién puede acceder a las instalaciones físicas donde se almacenan los datos.

5.3 Monitorización y supervisión: Describe cómo se monitorizan las instalaciones físicas.

**Gestión de incidentes**

6.1 Reporte y respuesta a incidentes: Define cómo se reportarán y responderán los incidentes.

6.2 Investigación de incidentes: Describe cómo se investigarán los incidentes.

6.3 Notificación de incidentes: Establece cuándo y cómo se notificarán los incidentes a las partes interesadas.

6.4 Gestión de la continuidad del negocio: Describe cómo se mantendrá el negocio en funcionamiento en caso de un incidente.

**Cumplimiento legal y contractual**

7.1 Cumplimiento legal y reglamentario: Asegura que todas las políticas cumplen con las leyes y regulaciones aplicables.

7.2 Conformidad con las políticas y procedimientos internos: Asegura que todas las políticas están en línea con cualquier política o procedimiento interno existente.

7.3 Revisión periódica y auditoría: Establece un proceso para revisar periódicamente las políticas y realizar auditorías.

7.4 Gestión de riesgos: Describe cómo se gestionarán los riesgos asociados con la seguridad de la información.

**Capacitación y concienciación**

8.1 Programa de formación y capacitación: Establece un programa para formar al personal sobre estas políticas.

8.2 Concientización de los empleados: Asegura que todos los empleados estén conscientes de estas políticas.

8.3 Pruebas de simulación de ataques: Realiza pruebas periódicas para asegurarse de que las políticas son efectivas.

**Políticas de respaldo y recuperación**

9.1 Copias de seguridad de los datos: Define cuándo y cómo se realizarán las copias de seguridad.

9.2 Procedimientos de recuperación ante desastres: Establece un plan para recuperarse en caso de un desastre.

9.3 Pruebas de recuperación ante desastres: Realiza pruebas periódicas para asegurarse de que el plan es efectivo.

**Políticas de teletrabajo**

10.1 Normas y estándares de seguridad de la información para el teletrabajo: Si los empleados trabajan a distancia, establece políticas para garantizar la seguridad.

10.2 Acceso remoto seguro: Define cómo los empleados pueden acceder de forma segura a los sistemas desde casa.

10.3 Protección de los dispositivos de trabajo: Establece políticas para proteger los dispositivos que se utilizan para el trabajo.

**Disposiciones finales**

11.1 Aprobación y actualización de la política: Define quién puede aprobar y actualizar la política.

11.2 Divulgación de la política: Describe cómo se comunicará la política a todas las partes interesadas.

11.3 Consecuencias de incumplimiento de la política: Establece las consecuencias para aquellos que no cumplan con la política.

11.4 Evaluación y mejora continua del sistema de gestión de seguridad de la información: Establece un proceso para evaluar y mejorar continuamente las políticas