**Introducción**

Las políticas de seguridad constituyen un pilar fundamental en la protección de los datos dentro de un sistema de información. A través de ellas se establece un proceso claro y detallado sobre cómo se deben abordar las medidas de seguridad en la empresa, especificando su correcta aplicación y el camino que se debe seguir para su implementación. En este documento se describirán las políticas a adoptar, junto con las estrategias de prevención y mitigación ante posibles incidentes de seguridad. Además, se definirá la asignación de roles a los empleados, de modo que cada uno pueda cumplir adecuadamente con sus responsabilidades.

**Propósito**

El objetivo de estas políticas es garantizar un entorno seguro y ordenado en la empresa, asegurando el correcto funcionamiento de sus sistemas. Las políticas permiten identificar y controlar actividades inseguras que podrían comprometer los datos críticos de la organización. Es importante destacar que estas políticas son obligatorias; sin ellas, la empresa no podría considerarse como tal en términos de seguridad informática, ya que son esenciales en cualquier acción que se lleve a cabo.

**Alcance**

SecureSoft no se limita a aplicar políticas de seguridad de manera interna, sino que su alcance está enfocado en la oferta de un amplio portafolio de servicios y soluciones en ciberseguridad para sus clientes. Entre los servicios que brinda se incluyen:

• Consultoría: Asistencia en el diseño e implementación de políticas de seguridad, incluyendo estándares como ISO 27001, y en la gestión de riesgos. • Seguridad ofensiva: Ejecución de pruebas de penetración (ethical hacking) para detectar vulnerabilidades.

• Seguridad defensiva: Vigilancia constante de amenazas (24/7) y respuesta ante incidentes.

• Implementación de soluciones: Instalación y configuración de herramientas de seguridad, como cortafuegos.

• Capacitación: Formación del personal en prácticas de ciberseguridad.

• Protección de datos: Asesoría sobre el cumplimiento de normativas de privacidad y protección de información

**Principios Fundamentales**

Para una correcta integración de las políticas de seguridad, es vital identificar claramente qué se necesita proteger: los datos. Estos deben cumplir con tres principios básicos de la ciberseguridad: confidencialidad, integridad y disponibilidad. Es decir, los datos deben estar protegidos contra accesos no autorizados, mantenerse íntegros sin alteraciones indebidas, y estar disponibles cuando se requieran. Solo el personal autorizado debe tener acceso a ellos, asegurando que la información esté siempre completa y segura.

|  |  |
| --- | --- |
| **Roles** | **Responsabilidades** |
| Consultor estrategico | Diseñar e implementar las politicas de seguridad de la empresa. |
| Auditor y evaluador | Realizar pruebas para identificar vulnerabilidades en la seguridad empresarial. |
| Operador de seguridad | Supervisar los eventos relacionados con la seguridad dentro de la organización. |
| Formador | Capacitar al personal sobre las politicas de seguridad establecidas. |
| Implementador tecnico | Actuar de forma inmediata ante incidentes de seguridad, minimizando su impacto. |
| Soporte continuo | Mejorar y actulizar los sistemas para asegurar su funcionamiento a futuro. |

**Clasificación de la Información**

**Categorías:**

* Confidencial: Incluye información altamente sensible como datos financieros, contratos legales, credenciales de sistemas, datos personales de clientes y empleados.
* Restringida: Comprende información técnica o de uso interno como código fuente, manuales de operación, documentación de proyectos, reportes internos.
* Pública: Información que puede ser divulgada sin afectar a la empresa, como el contenido del sitio web, material de marketing y publicaciones oficiales.

**Propósito:** Garantizar que la información sea manejada y protegida conforme a su nivel de sensibilidad, evitando accesos no autorizados y aplicando controles adecuados según su clasificación.

**7. Control de Acceso Medidas implementadas:**

* Autenticación Multifactor (MFA): Todos los usuarios deben autenticarse usando al menos dos métodos (por ejemplo, contraseña + código por aplicación móvil).
* Revisión periódica de permisos: Cada 6 meses se realiza una auditoría para verificar que los usuarios solo tengan los permisos necesarios para su rol.
* Registro de accesos fallidos: Se habilita un sistema de registros (logs) que documenta todos los intentos fallidos de acceso para detectar actividades sospechosas.

**Propósito:** Limitar el acceso a los recursos en función de los roles y responsabilidades de los empleados, reduciendo el riesgo de violaciones por privilegios innecesarios o mal uso de credenciales.

**8. Gestión de Incidentes de Seguridad**

**Acciones propuestas:**

* **Flujo de respuesta a incidentes:**

1. Detección y notificación inmediata del incidente.
2. Clasificación del tipo y nivel de impacto.
3. Contención y mitigación del incidente.
4. Investigación y análisis de causa raíz.
5. Documentación y aprendizaje.

* **Formulario de reporte de incidentes:** Incluye campos como tipo de incidente (p. ej., acceso no autorizado, malware), fecha y hora, área afectada, persona que reporta, descripción del evento, y acciones tomadas.

**Propósito:** Asegurar una respuesta eficiente y estructurada ante eventos de seguridad, minimizando el impacto y permitiendo la mejora continua del sistema.

**9. Política de Uso Aceptable**

**Directrices establecidas:**

* Actividades permitidas: Uso del correo electrónico institucional, acceso a sistemas autorizados, navegación en sitios relacionados con el trabajo.
* Actividades prohibidas: Instalación de software no autorizado, acceso a contenido inapropiado o ilegal, uso de dispositivos personales sin autorización, compartir contraseñas.

**Propósito:** Fomentar el uso responsable de los recursos tecnológicos de la empresa, garantizando que su utilización no comprometa la seguridad ni el funcionamiento de los sistemas.

**10. Gestión de Riesgos**

**Acciones implementadas:**

* Formulario de evaluación de riesgos: Para identificar y calificar amenazas, vulnerabilidades, impacto y probabilidad.
* Riesgos críticos identificados:

1. Acceso no autorizado a información sensible.
2. Pérdida de datos por fallos técnicos.
3. Ataques de malware/ransomware.
4. Errores humanos por falta de capacitación.
5. Fallos en proveedores externos.

* Planes de mitigación:
* Implementación de copias de seguridad automáticas.
* Aplicación de controles de acceso.
* Programas de capacitación.
* Auditoría a proveedores.
* Monitoreo continuo de amenazas.

**11. Formación y Concienciación**

**Actividad:**

* Elaboración de un cronograma de capacitación anual que incluya sesiones semestrales.
* Ejemplo: Capacitación “Reconociendo amenazas digitales: phishing y ransomware”.
* Simulaciones de phishing trimestrales con una meta del 80-90% de éxito en detección.
* Redacción y difusión de guías de buenas prácticas en el uso de contraseñas y navegación segura.

**Propósito:** Incrementar la conciencia de los empleados para evitar vulnerabilidades humanas y asegurar que sean la primera línea de defensa frente a amenazas.

**12. Gestión de Proveedores**

**Actividad:**

* Incluir cláusulas de seguridad en todos los contratos con proveedores (ej. obligación de cifrar datos sensibles).
* Realizar auditorías periódicas para revisar el cumplimiento de estas cláusulas.

**Propósito:** Garantizar que todos los proveedores cumplan con los estándares mínimos de seguridad requeridos por la organización.

**13. Auditorías y Revisión**

**Actividad:**

* Programar auditorías internas semestrales.
* Verificar configuraciones críticas como firewalls y logs de accesos.
* Evaluar políticas implementadas para identificar oportunidades de mejora.

**Propósito:** Evaluar periódicamente la efectividad de la Política de Seguridad de la Información (PSI) para realizar ajustes y mejoras continuas.

**14. Consecuencias del Incumplimiento**

**Actividad:**

* Definir un sistema de sanciones escalonado:
  + Primera infracción: Advertencia escrita.
  + Segunda infracción: Suspensión temporal.
  + Infracciones graves o reiteradas: Terminación del contrato laboral.

**Propósito:** Garantizar el cumplimiento de la PSI mediante medidas disciplinarias claras y conocidas por todo el personal.

**15. Referencias**

**Actividad:**

* Incluir una sección de referencias que contemple:
  + Normas internacionales como ISO/IEC 27001 (gestión de seguridad).
  + Legislación nacional/local, por ejemplo, la Ley de Protección de Datos Personales.

**Propósito:** Alinear la PSI con estándares reconocidos y normativas legales vigentes para asegurar su validez y aplicabilidad.