Documentación de Políticas y Procedimientos de Seguridad

1. Política de Seguridad

Propósito

La Universidad de California tiene como objetivo establecer un entorno seguro para proteger la información crítica y asegurar la continuidad de sus operaciones. Este propósito se basa en la adopción de estándares internacionales y mejores prácticas para la gestión de seguridad.

Principios clave

1. **Confidencialidad:**
    - Asegurar que solo las personas autorizadas tengan acceso a la información sensible.
    - Implementar controles como el cifrado de datos y políticas de acceso restringido.
2. **Integridad:**
    - Garantizar que los datos no sean alterados o manipulados de forma no autorizada.
    - Implementar sistemas de auditoría para detectar cambios no autorizados.
3. **Disponibilidad:**
    - Asegurar que la información esté accesible para los usuarios autorizados en cualquier momento.
    - Configurar sistemas de alta disponibilidad y planes de recuperación ante desastres.

Alcance

Esta política aplica a:

- **Sistemas tecnológicos:** Hardware, software y redes gestionadas por la universidad.
- **Datos:** Información académica, financiera y de investigación almacenada en sistemas internos o en la nube.
- **Usuarios:** Personal administrativo, docentes, investigadores, estudiantes y terceros autorizados.

Declaración de cumplimiento

La Universidad de California se compromete a cumplir con normativas y estándares aplicables como:

- **ISO/IEC 27001:** Gestión de seguridad de la información.
- **FERPA:** Protección de los derechos de los estudiantes.
- **HIPAA:** Seguridad de datos médicos.

2. Control de Acceso de Usuarios

Directrices generales

- **Asignación de accesos:**
  - Los permisos serán otorgados únicamente con base en la necesidad operativa y aprobados por el supervisor correspondiente.
- **Revisión de accesos:**
  - Accesos revisados trimestralmente para garantizar su adecuación al rol actual del usuario.
- **Revocación de accesos:**
  - Implementación inmediata al finalizar una relación laboral, académica o contractual.

Política de contraseñas

1. **Requisitos técnicos:**
   - Longitud mínima de 16 caracteres.
   - Incluir una combinación de letras mayúsculas, minúsculas, números y caracteres especiales.
   - Prohibido usar contraseñas basadas en información personal o palabras comunes.
2. **Gestión del ciclo de vida de contraseñas:**
   - Cambios obligatorios cada 90 días.
   - Prohibición de reutilización de contraseñas anteriores durante al menos los últimos 12 ciclos.
3. **Autenticación multifactor (MFA):**
   - Obligatoria para el acceso a sistemas críticos, implementada con tokens físicos o aplicaciones móviles de autenticación.

Gestión de privilegios

- **Principio de privilegios mínimos:**
    - Los usuarios tendrán únicamente los permisos necesarios para cumplir sus funciones.
- **Auditorías de permisos:**
    - Realización de auditorías trimestrales para identificar accesos no autorizados o excesivos.

3. Plan de Respuesta a Incidentes

Definición de incidente

Un incidente de seguridad es cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información. Esto incluye:

- Accesos no autorizados a sistemas críticos.
- Ataques cibernéticos como ransomware, phishing o DDoS.
- Pérdida, robo o destrucción de dispositivos con información sensible.
- Configuraciones incorrectas que permitan brechas de seguridad.

Procedimiento paso a paso

1. **Identificación:**
    - Detección inicial mediante herramientas de monitoreo o reportes manuales de usuarios.
    - Clasificación del incidente según su criticidad (alto, medio, bajo).
2. **Notificación:**
    - Informar al Equipo de Respuesta a Incidentes (IRT) dentro de los primeros 15 minutos.
    - Documentar el incidente en un sistema de gestión.
3. **Contención:**
    - Aislar los sistemas afectados del resto de la red.
    - Activar medidas temporales para detener la propagación del impacto.
4. **Investigación:**
    - Realizar análisis forense para determinar la causa raíz y el alcance del daño.
    - Identificar vulnerabilidades explotadas.
5. **Mitigación:**

    - Implementar parches, ajustes de configuración o restauraciones desde copias de seguridad.
6. **Cierre:**
    - Documentar el incidente, incluyendo lecciones aprendidas.
    - Actualizar políticas y controles para evitar recurrencias.

Roles y responsabilidades

- **IRT (Equipo de Respuesta a Incidentes):**
  Responsable de la identificación, contención y mitigación.
- **Usuarios finales:**
  Obligación de informar anomalías o incidentes sospechosos.

4. Copia de Seguridad y Recuperación de Datos

Procedimientos

1. **Automatización:**
    - Implementar sistemas automáticos para copias de seguridad.
    - Configurar respaldos incrementales diarios y completos semanales.
2. **Almacenamiento externo:**
    - Mantener una copia mensual en una ubicación fuera del sitio principal.
3. **Pruebas regulares:**
    - Realizar simulaciones de recuperación semestrales para garantizar la integridad de los datos.

Roles responsables

- **Administradores de sistemas:**
    - Monitorear y verificar la realización de respaldos según lo programado.
- **Auditores internos:**
    - Revisar informes de respaldos para detectar posibles inconsistencias.

5. Concienciación y Capacitación de los Empleados

Plan de capacitación

1. **Sesiones iniciales:**
    - Formación obligatoria para nuevos empleados sobre políticas de seguridad.
2. **Actualizaciones periódicas:**
    - Talleres trimestrales sobre ciberseguridad.
3. **Simulaciones:**
    - Pruebas regulares para evaluar la preparación ante amenazas como ataques de phishing.

Materiales de concienciación

1. **Boletines informativos:**
    - Envío mensual con actualizaciones de seguridad y consejos prácticos.
2. **Carteles:**
    - Colocados en lugares estratégicos con recordatorios de mejores prácticas de seguridad.

6. Aprobación y Revisión de Documentos

Proceso de aprobación

1. **Revisión inicial:**
    - El Comité de Seguridad evalúa todas las políticas y procedimientos antes de su implementación.
2. **Aprobación final:**
    - Firmada por el director del campus o el comité de gobernanza.

Revisión periódica

1. **Frecuencia:**
    - Todas las políticas serán revisadas anualmente.
2. **Revisiones extraordinarias:**
    - Tras incidentes significativos o cambios regulatorios.

Tabla Resumen del Informe

Sección	Descripción Breve	Puntos Clave
1. Política de Seguridad	Establece el compromiso de la universidad con la protección de la información.	Confidencialidad, Integridad, Disponibilidad, Cumplimiento de normativas (FERPA, HIPAA, ISO/IEC 27001).
2. Control de Acceso	Define cómo se otorgan, modifican y revocan los accesos de los usuarios.	Privilegios mínimos, autenticación multifactor, auditorías trimestrales, política de contraseñas robustas.
3. Plan de Respuesta a Incidentes	Describe cómo gestionar incidentes de seguridad de forma estructurada.	Identificación, Notificación, Contención, Mitigación, Documentación y Roles específicos del IRT.
4. Copia de Seguridad	Procedimientos para garantizar la disponibilidad y recuperación de datos.	Respaldos diarios y semanales, pruebas semestrales, almacenamiento externo cifrado.
5. Concienciación y Capacitación	Estrategias para formar al personal y fomentar una cultura de ciberseguridad.	Talleres trimestrales, simulaciones, carteles informativos, boletines mensuales.
6. Aprobación y Revisión	Define cómo se revisan, aprueban y actualizan las políticas de seguridad.	Revisión anual obligatoria, revisiones extraordinarias tras incidentes o cambios regulatorios.