SGSI de la Universidad de California

Sistema de gestión de la seguridad de la información (SGSI) para la Universidad de California.

Camila Aranibar Pozo

Tema 28: ISO 27001

Proyecto de desarrollo de un SGSI básico para una organización pública

INTRODUCCIÓN

En el siguiente documento se desarrolla un Sistema de Gestión de la Seguridad de la Información (SGSI) para complementar la Política de seguridad de la información electrónica (IS-3) y el Programa de gestión de la seguridad de la información (ISMP) de la Universidad de California.

Dado que la IS-3 de la Universidad de California incorpora la norma ISO 27001, ISO 27002, PCI (Payment Card Industry), HIPAA y el NIST 800-171; El presente SGSI, seguirá las especificaciones de los controles CIS (Center for Internet Security) para el mantenimiento y mejora continua del SGSI. La aplicación de estas medidas aseguran el mantenimiento de la confidencialidad, la protección de la integridad y la garantización de la disponibilidad de la información y los recursos informáticos de la Universidad de California.

OBJETIVO

Establecer un marco y unas directrices claras que guíen a todas las sedes de la Universidad de California en el cumplimiento de:

- Reducir y gestionar el ciberriesgo.
- Proteger la información y la privacidad de los datos.
- Respaldar el correcto funcionamiento de los activos informáticos.
- Fomentar activamente un programa de concienciación de seguridad.
- Implementar mejoras continuas para seguir las normativas recientes y anticiparnos en la detección y mitigación de riesgos.

ALCANCE

El alcance de este SGSI incluye toda la información de las sedes de la Universidad de California, incluyendo pero no limitando a la infraestructura de tecnología de la información (TI), los sistemas informáticos, los sistemas de red y todos los recursos informáticos. Asimismo, se incluye toda la información independientemente de la forma que esté procesada, el medio que la contenga o su almacenamiento (ya sea de forma impresa o electrónicamente).

La aplicación de este alcance tiene en cuenta los siguientes aspectos:

- ## Identificación de activos de la información:

Conforme al IS-3 sección 8 “Gestión de Activos”, todos los activos de la información (tanto información institucional como los Recursos de IT) se deben identificar y analizar por los propietarios o responsables del activo con el fin de determinar su protección.

Para conseguir este fin, los responsables de los activos deben cumplir con el Estándar de Clasificación de Información Institucional y Recursos de TI, donde se determinan los niveles de protección y los niveles de disponibilidad que se asignan a los activos.

Estos niveles se utilizan para seleccionar los controles de seguridad requeridos y para impulsar procesos clave. El nivel de protección tiene 4 categorías (P1, P2, P3, P4) basadas en el impacto de divulgación que puede dar lugar a sanciones, multas e incumplimiento de obligaciones legales, donde el P1 es el mínimo y P4 el máximo. El nivel de disponibilidad tiene 4 categorías (A1, A2, A3, A4) basadas en el impacto de la pérdida de disponibilidad o servicio que puede incurrir en pérdidas financieras para la universidad, donde A1 es el mínimo y A4 el máximo.

A continuación se crea un inventario identificando y clasificando de los activos de la información siguiendo este Estándar de Clasificación de Información Institucional y Recursos de TI:

Activo	**Nivel de protección**	**Nivel de disponibilidad**
Ordenadores y portátiles	P3 - moderado	A3 - moderado
Móviles	P3 - moderado	A2 - bajo
Impresoras y escáneres	P2 - bajo	A2 - bajo
Teléfonos y centralitas	P3 - moderado	A4 - alto
Switches	P3 - moderado	A3 - moderado
Access Points	P4 - alto	A4 - alto
Firewalls	P3 - moderado	A4 - alto

WAF	P3 - moderado	A4 - alto
Base de datos	P4 - alto	A4 - alto
Servidores físicos o virtuales	P4 - alto	A4 - alto
Sistemas operativos	P3 - moderado	A4 - alto
Aplicaciones de gestión interna	P4 - alto	A4 - alto
Carpetas de red compartidas	P4 - alto	A4 - alto
Copias de seguridad	P4 - alto	P3 - moderado
Almacenamiento en la nube	P4 - alto	A4 - alto

- ## Límites físicos:

Este SGSI se aplica a todos los campus y centros médicos de la Universidad de California, la Oficina del Rector de la Universidad de California, el Departamento de Agricultura y Recursos Naturales de la Universidad de California, los laboratorios nacionales administrados por la Universidad de California y todas las demás sedes de la Universidad de California .

Adicionalmente, se determinan áreas de acceso restringido a todos los centros de datos o CPDs, laboratorios de investigación y salas de documentación confidencial que se encuentran en todas las ubicaciones descritas previamente.

- ## Límites virtuales:

A todos los servicios en la nube que estén contratados y que contengan información o activos de la Universidad de California, están dentro del alcance y se les aplica este SGSI. Asimismo, se incluyen las máquinas virtuales y sistemas de desarrollo o almacenamiento en cloud.

PARTES INTERESADAS - ROLES Y RESPONSABILIDADES

- **Consejo de Seguridad de la Información (ISC):** es el colectivo universitario de Directores de Seguridad de la Información (CISO), cuya responsabilidad es servir como órgano de consulta y asesoramiento en iniciativas de ciberseguridad para el CISO de todo el sistema, el Consejo de CIO, el Comité de Gobernanza de Riesgos Cibernéticos (CRGC), el Consejo de Rectores, el Presidente del Sistema y otros directivos de la Universidad de California.
- **Rectores, vicerrectores del sistema de salud, director del Laboratorio Nacional Lawrence Berkeley, UC, director de operaciones, vicepresidente de la División de Agricultura y Recursos Naturales:** Deben asignar a los responsables de implementar esta política en sus ubicaciones.
- **Ejecutivo/a responsable de riesgos cibernéticos (CRE):** Supervisa que todos los roles cumplan con sus funciones. También realiza evaluaciones de riesgo de seguridad de la información y del nivel de ciberriesgo, para gestionar los riesgos y asegurar la financiación.
- **Director de Seguridad de la Información de todo el Sistema:** Es responsable de garantizar la implementación uniforme de este sistema y de coordinar a los funcionarios de las sedes.
- **Chief Information Officer (CIO):** Se encarga de supervisar la gestión de la planificación, implementación, presupuesto, dotación de personal, desarrollo de programas y presentación de informes de seguridad de la información, todo alineado con las prioridades de la CRE.
- **Chief Information Security Officer (CISO):** Responsable de aplicar estrategias para garantizar el cumplimiento del ISMP y de las medidas de seguridad.
- **Equipo de auditoría interno:** equipo especializado en la supervisión del cumplimiento de los controles del SGSI una vez implementado.
- **Personal y alumnos:** Debe cumplir con todas las directrices del SGSI. No se aplica a los estudiantes que no sean miembros del personal interno.
- **Equipo de IT:** Debe colaborar en la implementación de todas las mejoras de seguridad en los recursos informáticos para el cumplimiento del SGSI.
- Proveedores o Externos: Se deben alinear con la visión y directrices del SGSI, cumpliendo con los controles asignados y los requisitos establecidos en los contratos de servicios.

EVALUACIÓN DE RIESGOS

Este apartado es fundamental en el SGSI, ya que gracias a la evaluación de riesgos se pueden identificar amenazas, priorizar su mitigación y realizar medidas de mejora de la seguridad de los activos. De esta forma se puede tener una visibilidad completa para realizar los planes o estrategias de mejora y definir los controles que se seguirán.

Conforme al IS-3 sección 6 “Proceso de Gestión de Riesgos”, todas las sedes de la Universidad de California deben realizar evaluaciones de riesgo basados en los controles y requisitos establecidos, donde se detallan los mínimos de evaluación y gestión del riesgo. Además, las sedes pueden añadir requisitos adicionales para cumplir con la tolerancia de riesgo y según consideren necesario.

Se realizará una identificación y evaluación de los riesgos asociados a los activos de la Universidad de California. Para ello se tendrá en cuenta: el IS-3 sección 6 explicado previamente, todas las categorías que definen al activo (hardware, software, datos), las posibles amenazas que puedan afectar a cada activo, las vulnerabilidades que podrían exponer los activos a las amenazas identificadas, la probabilidad de ocurrencia (alta, media, baja) de cada riesgo, el impacto en la Universidad de California en caso que se produzca el riesgo. Finalmente, en base a todos estos parámetros se definirá una calificación de riesgos (alto, medio, bajo) para priorizar aquellos riesgos que se deben mitigar inmediatamente.

Activo	**Categoría**	**Amenazas potenciales**	**Vulnerabilidades**	**Probabilidad**	**Impacto**	**Riesgo**
Ordenadores y portátiles	Hardware, software y datos	1) Malware (virus, troyanos, ransomware) 2) Acceso no autorizado 3) Pérdida o robo físico 4)Vulnerabilidades de software desactualizad	1) Sistemas operativos sin parches de seguridad 2) Antivirus desactualizado o no instalado 3) Contraseñas débiles o compartidas 4) Configuraciones inseguras (ej. RDP	Alta	1) Pérdida o robo de información confidencial 2) disminución de productividad del usuario afectado	Alto

		o 5) Phishing 6) Uso indebido por parte de empleados	abierto sin control o puertos UBS accesibles). 5) Cifrado de disco no realizado 6) Falta de políticas de navegación mediante un Firewall o Proxy web			
Móviles	Hardware, software y datos	1) Pérdida o robo del dispositivo 2) Acceso no autorizado a datos corporativos 3) Aplicaciones maliciosas 4) Conexiones a redes WiFi no seguras 5) Falta de cifrado en comunicaciones o almacenamiento	1) Falta de autenticación y contraseña de acceso 2) Aplicaciones no autorizadas instaladas 3) Sistema operativo no actualizado 4) Falta de implementación de MDM (Mobile Device Management).	Media	1) Filtración de datos y consecuencias legales si se comprometen datos sensibles y personales	Alto
Impresoras y escáneres	Hardware y software	1) Acceso no autorizado a documentos impresos o escaneados 2) Intercepción de trabajos de impresión en red 3) Firmware vulnerable o no actualizado	1) Firmware sin actualizar 2) Contraseñas por defecto o falta de autenticación 3) Interfaz web de administración sin protección de credenciales 4) Servicios innecesarios habilitados en los puertos donde se	Baja	1) Filtración de información confidencial 2) Posibles daños reputacionales en caso que un atacante entre a la red interna mediante el	Bajo

		4) Mala protección de la red que permita puntos de entrada	conecta la impresora		acceso de una impresora	
Teléfonos y centralitas	Hardware y software	1) intercepción de llamadas 2) Ataques de denegación de servicio (DoS) 3) Suplantación de identidad utilizando el mismo número 4)Vulnerabilidades en la centralita o en el sistema VoIP	1) Interfaces de administración expuestas externamente sin seguridad e internamente sin credenciales de acceso 2) Configuración de protocolos inseguros (ej. SIP sin cifrado). 3) Configuración por defecto no modificada (sin alterar las extensiones y derivaciones) 4) Falta de monitorización de llamadas. 5) Red VoIP sin segmentación adecuada con su Vlan específica	Media	1) Daños reputacionales por la pérdida de confianza de clientes y proveedores 2) Pérdidas financieras ya que en caso de que las líneas telefónicas están inoperativas no se realizan pago de las reservas de matrículas 3) Compromiso de datos sensibles en caso que las llamadas sean escuchadas	Medio
Switches	Hardware y software	1) Acceso no autorizado a la red 2) Ataques de red como ARP spoofing, MAC flooding 3) Mala e insegura configuración	1) Gestión mediante protocolos inseguros (ej. Telnet, HTTP). 2) Contraseñas por defecto o sin cambiar para acceder a la configuración del	Media	1) En caso de estar inoperativos, la interna no funcionaria y se produciría una pérdida financiera	Alto

		(no configurando las vlans correctamente) 4) Firmware desactualizado	SW 3) Falta de control de acceso por VLAN o ACLs. 4) Firmware sin parches y sin actualizar 5) SNMP abierto o mal configurado			
Access Points	Hardware, software y datos	1) Ataques de fuerza bruta a la contraseña 2) Acceso no autorizado desde redes inalámbricas 3) Poner puntos de acceso falsos que no son de la Universidad	1) WiFi con cifrado débil (WEP/WPA). 2) Contraseña de administración de los AP por defecto 3) Falta de autenticación 802.1X 4) SSID visibles innecesarios (como los de pruebas) y mal segmentados 5) Firmware desactualizado 6) Falta del control e inventario de los AP de la Universidad, ya que sino no se podrán detectar los APs no autorizados	Alta	1) Daños reputacionales si un atacante accede a la red interna mediante un AP 2) Compromiso de datos sensibles y corporativos	Alto
Firewalls	Hardware y software	1) Configuración incorrecta o excesivamente permisiva 2) Ataques de denegación de servicio (DDoS) 3) Firmware desactualizad	1) Reglas mal configuradas o laxas 2) Interfaces de gestión accesibles desde internet 3) Contraseñas de acceso débiles o manteniendo la que viene por defecto	Media	1) Filtración de datos hacia el exterior 2) Pérdidas financieras si los servicios no están operativos	Alto

		o y vulnerable 4) Desactivación accidental de reglas ya establecidas	4) Falta de segmentación interna 5) Desactivación accidental de las reglas implementadas			
WAF	Hardware y software	1) Reglas mal configuradas que bloquean tráfico legítimo 2) Fallos en la integración con aplicaciones web 3) Ataques de denegación de servicio (DDoS) 4) Ataques web nuevos de tipo 0-day	1) Reglas genéricas o mal configuradas 2) Falta de integración con el SIEM o las alertas.	Media	1) Filtración de datos hacia el exterior 2) Pérdidas financieras si los servicios no están operativos	Medio
Base de datos	Hardware, software y datos	1) Inyección SQL 2) Acceso no autorizado 3) Pérdida de integridad, disponibilidad o confidencialidad de los datos almacenados 4) Falta de cifrado en reposo o en tránsito 5) Fugas de información	1) Inyección SQL por falta de validación 2) Accesos con cuentas con demasiados privilegios 3) Base de datos accesible desde el exterior 4) Falta de cifrado de datos 5) Falta de monitorización de los acceso y de las consultas en las tablas 6) Violación de datos	Alta	1) Pérdidas financieras ya que no se podrá acceder a los datos de esa BBDD 2) Daños reputacionales por la pérdida de confianza de clientes y proveedores 3) Compromiso de datos sensibles que pueden dar	Alto

					lugar a sanciones o multas	
Servidores físicos o virtuales	Hardware, software y datos	1) Ataques de ransomware 2) Accesos remotos no controlados - accesos no autorizados 3) Desactualizaciones que den lugar a la explotación de vulnerabilidades 4) Fallos de hardware 5) Escalación de privilegios	1) Puertos abiertos innecesariamente 2) Servidores sin parchear 3) Usuarios con demasiados privilegios 4) Falta de políticas de hardening del sistema 5) Falta de monitorización de los accesos a los servidores 6) Mala configuración del RDP que permite acceso a todos	Alta	1) Pérdidas financieras ya que los servicios no estarán operativos	Alto
Sistemas operativos	Software y datos	1) Mal uso de permisos de usuario 2) Instalación de software no autorizado 3) Desactualizaciones que den lugar a la explotación de vulnerabilidades	1) Sistemas sin parches de seguridad 2) Servicios innecesarios habilitados 3) Configuraciones por defecto no ajustadas 4) Autenticación débil o sin el 2FA	Alta	1) Pérdidas financieras ya que los servicios no estarán operativos	Alto
Aplicaciones de gestión interna	Software y datos	1) Usuarios con privilegios excesivos 2) Inyecciones de código 3) Filtración de	1) Accesos sin control de privilegios por rol y grupo de AD 4) Fallos en disponibilidad de la aplicación por	Alta	1) Pérdidas financieras ya que los servicios no estarán operativos 2) Daños	Alto

		información sensible 4) Programaciones inseguras que no sigan las directrices del OWASP	errores en el código fuente 5) Exposición de código y de información interna al exterior por mala configuración del software		reputacionales por la pérdida de confianza de clientes y proveedores	
Carpetas de red compartidas	Software y datos	1) Acceso no autorizado debido a la mala segmentación de las carpetas 2) Usuarios con privilegios excesivos 3) Eliminación o modificación accidental o maliciosa de los archivos 4) Ransomware cifrando archivos 5) Falta de control de versiones o registros de acceso	1) Falta de restricción de permisos de acceso 2) Falta de backups realizados frecuentemente 3) No se realiza cifrado en el tránsito 4) Violación de datos	Media	1) Pérdidas financieras ya que los servicios no estarán operativos 2) Daños reputacionales por la pérdida de confianza de clientes y proveedores	Alto
Copias de seguridad	Hardware, software y datos	1) Copias mal almacenadas 2) Copias sin cifrar los datos en reposo 3) No realización de pruebas de restauración 4) Pérdida o	1) El almacenamiento de copias no tiene separación de lógica ni de red 2) Las copias no están cifradas 3) Falta de realización de pruebas de restauración	Media	1) Compromiso de datos que puede derivar a sanciones por incumplimiento del periodo de retención de datos	Alto

		robo de las copias 5) Ransomware afectando también las copias 6) Desactualización del sistema de copias 7) Accesos no autorizados	planificadas y recurrentes. 4) Monitorización de los accesos y logs 5) Software de de las copias desactualizado 6) Violación de datos			
Almacenamiento en la nube	Software y datos	1) Accesos no autorizados y/o no controlados 2) Fugas de datos 3) Dependencia del proveedor 4) Almacenamiento sin cifrar	1) Ausencia de cifrado de datos, tanto en tránsito como en reposo 2) Cuentas con autenticación débil o sin 2FA. 3) Violación de datos	Alta	1) Pérdidas financieras ya que los servicios no estarán operativos 2) Daños reputacionales por la pérdida de confianza de clientes y proveedores	Alto

SELECCIÓN DE CONTROLES

Dado que la Política de seguridad de la información electrónica (IS-3) de la Universidad de California ya incorpora controles de la ISO27001, ISO27002, HIPAA, PCI y NIST 800-171); en este apartado seleccionaremos los controles apropiados para mitigar los riesgos identificados y se basarán en los controles CIS (Center for Internet Security). Los controles CIS están organizados en 18 grupos que ayudan a fortalecer la ciberseguridad en función del riesgo.

Para la mitigación de los riesgos altos, realizamos una priorización de controles de seguridad alineados con los controles CIS versión 8.0. Los controles CIS recomendados segun el tipo de activo previamente analizado son los siguientes:

1. Base de datos

- **CIS 4 - Secure Configuration of Enterprise Assets:** Aplicar configuraciones seguras y eliminar configuraciones por defecto.
- **CIS 6 - Access Control Management:** Minimizar privilegios, uso de cuentas separadas para admins y priorizar cuantas nominales.
- **CIS 8 - Audit Log Management:** Registrar todas las acciones en la base de datos y monitorizar accesos.
- **CIS 10 - Malware Defenses:** Escaneo de bases de datos y conexiones por malware.
- **CIS 12 - Network Infrastructure Management:** Asegurar segmentación de red para aislamiento correcto de los activos.

2. Servidores físicos y virtuales

- **CIS 4 - Secure Configuration:** Aplicar plantillas de hardening (ej. CIS Benchmarks) para las configuraciones seguras.
- **CIS 5 - Account Management:** Control estricto de cuentas de administración.
- **CIS 7 - Security Awareness and Skills Training:** Capacitar y conciencias a los usuarios admins sobre buenas prácticas.
- **CIS 11 - Data Recovery:** Verificar las copias de seguridad y hacer pruebas frecuentes para asegurar que funcionan correctamente
- **CIS 14 - Security Operations Center (SOC) Functions:** Monitorización y respuesta a incidentes.

3. Sistemas operativos

- **CIS 3 - Data Protection:** Cifrado de datos en reposo y en tránsito.
- **CIS 4 - Secure Configurations:** Deshabilitar servicios y puertos innecesarios.
- **CIS 10 - Malware Defenses:** Asegurarse que el antimalware y antivirus están actualizados y activos.
- **CIS 16 - Application Software Security:** Aplicar parches de seguridad periódicamente.
- **CIS 13 - Security Service Provider Management:** Controlar y gestionar de forma segura los servicios externos.

4. Aplicaciones de gestión interna

- **CIS 16 - Application Software Security:** Realizar validación de entradas, pruebas de seguridad y asegurarse que se realiza un ciclo de vida de desarrollo de software seguro.
- **CIS 6 - Access Control Management:** Garantizar que los roles y permisos tienen mínimos privilegios.

- **CIS 3 - Data Protection:** Cifrado y protección de la información sensible.
- **CIS 14 - Security Operations Center Functions:** Monitorización de logs de aplicaciones críticas.

5. Carpetas de red compartidas

- **CIS 3 - Data Protection:** Controlar el acceso a carpetas por usuario, permisos y rol, aplicando el principio de minimo privilegio y el principio de conocer.
- **CIS 6 - Access Control Management:** Aplicar el principio de mínimo privilegio.
- **CIS 11 - Data Recovery:** Realizar copias recurrentes y recuperaciones automáticas.
- **CIS 9 - Email and Web Browser Protections:** Prevención de ransomware que use rutas compartidas.

6. Almacenamiento en la nube

- **CIS 3 - Data Protection:** Cifrar los datos en tránsito y en reposo.
- **CIS 5 - Account Management:** Gestionar los accesos con MFA.
- **CIS 6 - Access Control Management:** Revissar y ajustar de permisos en los contenedores o copias.
- **CIS 15 - Wireless Access:** Validar las políticas de accesos desde móviles/remoto.
- **CIS 13 - Service Provider Management:** Evaluar seguridad del proveedor cloud.

7. Firewalls

- **CIS 12 - Network Infrastructure Management:** Gestión segura y revisión periódica de reglas.
- **CIS 4 - Secure Configuration:** Seguir guías de hardening para los dispositivos de red.
- **CIS 8 - Audit Log Management:** Registrar los cambios y accesos al firewall.
- **CIS 14 - SOC Functions**: Crear alertas de tráfico inusual.

8. Access Points (WiFi)

- **CIS 15 - Wireless Access Control:** Utilizar WPA3 o mínimo WPA2 con autenticación 802.1X.
- **CIS 6 - Access Control:** Segmentar las redes como mínimo en red de invitados, red dispositivos IoT y red corporativa.
- **CIS 4 - Secure Configuration:** Cambiar las credenciales por defecto y mantener actualizado el firmware.

9. Switches

- **CIS 12 - Network Infrastructure Management:** Segmentar las redes por VLAN y bloquear los puertos innecesarios.
- **CIS 4 - Secure Configuration:** Configurar de forma segura los switch (SNMP, Telnet, etc.).
- **CIS 8 - Logging:** Monitorizar los eventos de los switches para poder detectar anomalías.

10. Ordenadores, portátiles y móviles

- **CIS 1 - Inventory of Enterprise Assets:** Registrar todos los dispositivos de forma adecuada cumpliendo unos parámetro minimos (nombre del activo, proveedor, localización del activo…).
- **CIS 2 - Software Inventory:** Controlar el software instalado mediante un inventario actualizado.
- **CIS 7 - Security Awareness Training:** Formar sobre las buenas prácticas de ciberseguridad a todos los empleados, como por ejemplo las tácticas de phishing.
- **CIS 10 - Malware Defenses:** Activar el antimalwarare o EDR en todos los activos.
- **CIS 5 - Account Management:** Aplicar políticas de contraseñas fuertes, con 2FA y que su periodo de renovación sea de 90 días.

Planificación de la implementación

Es fundamental crear un Plan de Implementación de los Controles CIS seleccionados previamente, ya que así aseguramos que se adoptan de forma efectiva en la Universidad de California. A continuación detallamos el cronograma y los recursos necesarios para la implementación de los controles:

- **A corto plazo:** En este periodo de máximo 3 meses se implementarán los controles CIS 4, CIS 6, CIS 10, CIS 3. Se prioriza mitigar las amenazas de los activos de bases de datos, servidores, almacenamiento en la nube y carpetas compartidas.
- **A medio plazo:** En un periodo de 3 a 6 meses se implementarán los controles CIS 5, CIS 12, CIS 11, CIS 8. Durante este periodo nos focalizamos en los controles de infraestructura y recuperación.
- **A largo plazo:** Este peridod es de 6 a 12 meses, donde se implementarán los controles CIS 1, CIS 2, CIS 7, CIS 16, CIS 15, CIS 13, CIS 14. Estos controles fortalecerán la infraestructura, los procesos y la concienciación del personal.

Los recursos necesarios para la implementación de estos controles son:

- **Personal:** personal interno del departamento de informática y la colaboración de otros departamentos cuando sea necesario para realizar pruebas, etc
- **Herramientas informáticas:** SIEM, sistema de copias, escaner de vulnerabilidades, plataforma de concienciación y formación, antivirus.
- **Formación:** Personal encargado de formar a los técnicos y al resto de personal sobre la concienciación en seguridad.
- **Financiación:** recursos financieros necesarios para implementar todas las herramientas y mejoras.

DOCUMENTACIÓN DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD

La Política de seguridad de la información electrónica (IS-3) de la Universidad de California, concretamente la sección III, dispone de 18 subsecciones donde se explican las políticas.

Adecuandonos a este IS-3 ya implementado, a continuación complementaremos las políticas definidas para mejorar la prácticas de seguridad:

Política de Seguridad

Conforme a la IS-3 sección 1, un Programa de Gestión de Seguridad de la Información (ISMP) es un requisito fundamental para proteger la confidencialidad, integridad y disponibilidad de la Información Institucional y los Recursos IT de la Universidad de California.

Para conseguir este objetivo, el programa se basará en los controles definidos en la IS-3 y adicionalmente, en los controles CIS propuestos en este documento SGSI. Todos los requisitos y controles de seguridad serán aplicados en todas las sedes y con la colaboración activa de las partes interesadas. Por tanto la universidad de California se compromete a:

- Promover las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación de la política entre el personal.
- Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.

- ## Control de Acceso de Usuarios

Conforme a la IS-3 sección 9, las sedes deben garantizar que el acceso a la Información Institucional se ajuste a los principios de necesidad de saber y mínimo privilegio. Se tienen que implementar controles adicionales para el acceso a la información clasificada como confidencial o sensible. Solo el personal autorizado debe acceder mediante un usuario único y con los permisos aprobados y necesarios para desempeñar sus funciones.

Las contraseñas deben cumplir con unos mínimos de seguridad: longitud mínima de 12 caracteres, inclusión de caracteres especiales y alfanuméricos, renovación de las contraseñas cada 90 días, no utilización de las últimas 5 contraseñas. Adicionalmente se implementarán 2FA para el acceso a aquellos recursos que contengan datos sensibles o personales.

- ## Plan de Respuesta a Incidentes

Conforme a la IS-3 sección 16, la gestión de incidentes requiere una respuesta rápida, eficaz y ordenada. Por lo que cada sede debe implementar un plan de respuesta ante incidentes atendiendo a sus necesidades específicas. No obstante, todos los planes de respuesta ante incidentes deben tener las 5 fases definidas:

1. **Preparación:** Todo el personal debe estar consciente de los pasos que debe seguir en caso de incidente.
2. **Detección, investigación y análisis:** Todos los empleados y los estudiantes deben notificar los incidentes. Los gerentes del equipo y los jefes de unidad deben informar de inmediato al CISO sobre los incidentes de seguridad de la información.
3. **Contención y mitigación:** los equipos técnicos deben coordinarse para contener el incidente, recolectar evidencias y mitigar para reducir la afectación.
4. **Recuperación:** Los equipos técnicos tienen que restablecer los equipos afectados para que estén operativos.
5. **Aprender y mejorar:** Se tiene que aprender de todas las experiencias para tomar acciones de mejora e implementar nuevos controles.

Para la gestión del incidente los roles involucrados son:

- **Personal y alumnos:** deben informar de cualquier incidente
- **Departamento de IT:** todo el equipo de informática se debe coordinar para gestionar el incidente en el menor tiempo posible
- **Departamento de comunicación:** debe estar preparado en caso extremo de tener que realizar un comunicado de prensa

- ## Copia de Seguridad y Recuperación de Datos

Conforme a la IS-3 sección 12, las sedes deben garantizar que la información institucional clasificada con un nivel de disponibilidad 3 o superior esté respaldada y sea recuperable. También deben conservar adecuadamente las copias y hacer pruebas de recuperación para garantizar la eficacia y que cumplen con todos los requisitos.

Las copias de seguridad se deben realizar de forma recurrente y automatizada, combinando las copias de tipo full y las copias de tipo incremental. El almacenamiento de las copias debe variar dependiendo de si es a largo plazo o a corto plazo y se debe priorizar la deslocalización de su almacenamiento. De esta forma se podrá prevenir la pérdida de datos por incidentes naturales.

- ## Concienciación y Capacitación de los Empleados

Conforme a la IS-3 sección 5.2.3, todas las sedes deben implementar capacitación, campañas de concientización, materiales educativos y otras iniciativas para garantizar que todos los miembros del personal comprendan los riesgos de seguridad, las buenas prácticas y sus roles y responsabilidades.

Se promoverá que todo el personal participe activamente en las formaciones como mínimo dos veces al año y los alumnos como mínimo una vez al año. Dado que cada sede elige su plan de formación, se debe incluir como mínimo los siguientes temas: métodos actuales de phishing, buenas prácticas de teletrabajo, aviso de incidentes, adecuada utilización y manejo de datos personales y confidenciales, buenas prácticas básicas (no dejar la contraseña escrita en post it, bloquear el ordenador cuando no estás en tu puesto de trabajo…)

- ## Aprobación y Revisión de Documentos

Conforme a la IS-3 sección 2.3, la gestión de la seguridad de la información requiere una combinación de políticas y estándares. Las sedes pueden desarrollar y aprobar políticas, estándares, procedimientos, directrices de apoyo, listas de verificación de apoyo y mejores prácticas específicas a fin de explicar los requisitos y métodos específicos de la IS-3. Los documentos de apoyo pueden ser más restrictivos que el IS-3, pero no menos restrictivos.

Todas las políticas, normativas, etc de cada sede se deben aprobar por el CISO de la sede. Asimismo se actualizarán cuando se produzcan cambios significativos en la infraestructura o avances tecnológicos o como mínimo cada 2 años.