Desarrollo de Sistema de Gestión de Seguridad de la información.

Objetivo del SGSI de UCOP

En este proyecto de desarrollo de un SGSI Básico, elegí el Sistema de la Universidad de California. El objetivo principal del SGSI de UCOP es proteger la **confidencialidad, integridad y disponibilidad** de la información crítica que maneja la organización. Esto incluye garantizar la seguridad de los datos personales, financieros y de investigación, además de cumplir con las normativas legales y regulatorias relevantes, como la **FERPA** para información de estudiantes y la **HIPAA** para datos médicos de pacientes, entre otras.

1.- Definición de Alcance.

Inventario de Activos de Información de UCOP:

En el inventario de activos de información para el SGSI de la UCOP, basado en la página https://security.ucop.edu/index.html, podemos identificar varios tipos de activos clave. Estos activos se pueden clasificar de la siguiente manera:

1. Hardware:

- **Computadoras:** Portátiles y de escritorio utilizadas por empleados, académicos y personal administrativo.
- **Servidores:** Servidores locales y en la nube que albergan datos de estudiantes, académicos y datos administrativos.
- **Dispositivos de red:** Routers, firewalls y switches que soportan la conectividad de la red institucional.
- **Sistemas de almacenamiento:** Dispositivos de almacenamiento en red (NAS), unidades de almacenamiento externas y discos duros internos.
- **Equipos de laboratorio:** Hardware especializado utilizado en investigaciones académicas, incluyendo dispositivos biométricos o sensores conectados.

2. Software:

- **Sistemas Operativos:** Windows, macOS, Linux, y otros sistemas operativos utilizados en la infraestructura UCOP.
- **Sistemas de gestión de información:** Software que administra la información de estudiantes, empleados y ciudadanos, como PeopleSoft.

- **Aplicaciones en la nube:** Herramientas como Google Workspace, plataformas de colaboración en la nube y sistemas de almacenamiento como AWS o Azure.
- **Software académico y administrativo:** Aplicaciones especializadas para la gestión de proyectos de investigación, aprendizaje a distancia (LMS), y sistemas financieros.

3. Datos:

- **Información personal (PII):** Datos de identificación de estudiantes, empleados, pacientes y ciudadanos.
- **Datos financieros:** Información relacionada con la contabilidad, nómina, y presupuestos operativos de la universidad.
- **Datos de investigación:** Propiedad intelectual, estudios y análisis realizados por el personal académico y de investigación.
- **Datos de salud:** Información médica de pacientes que participan en proyectos de investigación o están afiliados al sistema de salud UCOP.

4. Infraestructura en la nube:

- **Plataformas en la nube:** Servicios en la nube contratados como parte de la infraestructura de almacenamiento y procesamiento, que pueden incluir AWS, Azure, y Google Cloud.
- **Máquinas virtuales:** Servidores virtuales que ejecutan aplicaciones críticas o servicios web internos.

5. Personal:

- **Administradores de sistemas:** Personal de TI encargado de la gestión y operación de la infraestructura.
- **Académicos e investigadores:** Usuarios que acceden a los sistemas de información para gestionar proyectos y acceder a datos de investigación.
- **Empleados administrativos:** Personal que accede a los sistemas de gestión de recursos humanos, nómina, y otros servicios administrativos.

Clasificación de Activos según su Importancia para las Operaciones:

- **Crítico:**
    - Servidores de bases de datos que contienen PII y datos de investigación.
    - Infraestructura de red (routers, firewalls) que protege y gestiona la conectividad.
    - Datos financieros y de nómina.

- **Alto:**
    - Sistemas operativos y aplicaciones de gestión de estudiantes y académicos.
    - Sistemas de salud y de información administrativa.
- **Medio:**
    - Equipos de cómputo personal y software general.
    - Correo electrónico institucional.
- **Bajo:**
    - Sistemas de colaboración interna de bajo impacto, como foros y plataformas de mensajería no crítica.

Este inventario es fundamental para garantizar que todos los activos se protejan de acuerdo con su nivel de criticidad dentro del SGSI.

Límites Físicos del SGSI de UCOP:

Basado en la página de UCOP (https://security.ucop.edu/index.html), los límites físicos para el Sistema de Gestión de Seguridad de la Información (SGSI) abarcan las siguientes ubicaciones:

Ubicaciones incluidas en el SGSI:

1. **Oficinas Administrativas:**
    - Las oficinas principales de la UCOP, donde se gestiona la administración y operación central de la universidad.
    - Oficinas ubicadas en Oakland y otras instalaciones satélite que forman parte del sistema UCOP.
2. **Centros de Datos:**
    - **Data Centers** donde se almacenan y procesan datos críticos, tanto locales como aquellos que se encuentran en la nube, incluyendo centros de respaldo.
    - Centros de datos ubicados en diferentes campus del sistema de la Universidad de California y cualquier instalación externa que forme parte de la infraestructura de TI.

3. **Campus Universitarios:**
    - Los campus que forman parte de la Universidad de California, ya que muchos de ellos están conectados al sistema UCOP y manejan información crítica de estudiantes, personal académico, investigación y más.
4. **Áreas Físicas de Investigación:**
    - Laboratorios e instalaciones de investigación que manejan datos sensibles o realizan experimentos con datos críticos relacionados con la propiedad intelectual y proyectos académicos.
5. **Otras Instalaciones:**
    - Centros de soporte técnico y oficinas descentralizadas que pueden manejar sistemas de almacenamiento y procesamiento de datos importantes para la infraestructura operativa.

Áreas que necesitan acceso restringido:

1. **Salas de Servidores:**
    - Ubicaciones dentro de los centros de datos donde se encuentran los servidores físicos y otros equipos de almacenamiento.
    - Estas áreas deben tener controles de acceso estrictos, como verificación biométrica y supervisión 24/7.
2. **Laboratorios de Investigación:**
    - Instalaciones donde se realizan investigaciones con datos altamente sensibles. Estas áreas requieren un control riguroso para prevenir el acceso no autorizado.
3. **Áreas Administrativas Críticas:**
    - Oficinas que manejan la gestión financiera, nómina o datos de estudiantes y empleados. Estas áreas deben estar restringidas solo al personal autorizado.
4. **Sitios de Respaldo y Recuperación de Desastres:**
    - Instalaciones físicas utilizadas para almacenar copias de seguridad de datos críticos. Estas áreas deben tener medidas adicionales de seguridad física para asegurar la integridad y disponibilidad de los datos.

Este límite físico asegura que las ubicaciones clave donde se manejan, almacenan o procesan los datos importantes estén adecuadamente protegidas dentro del SGSI, con un enfoque particular en la restricción de acceso y el monitoreo continuo de estas áreas críticas.

Límites Virtuales del SGSI de UCOP:

Basado en la página de UCOP (https://security.ucop.edu/index.html), los límites virtuales para el Sistema de Gestión de Seguridad de la Información (SGSI) de UCOP incluyen lo siguiente:

1. Redes Incluidas en el SGSI:

1. **Red Interna de UCOP:**
    - La red interna que conecta las oficinas administrativas y los campus que forman parte del sistema de la Universidad de California.
    - Esta red maneja la transferencia de datos críticos entre departamentos, estudiantes, personal académico, e investigadores.
2. **Redes Privadas Virtuales (VPN):**
    - VPNs utilizadas por el personal de UCOP para acceder de manera remota y segura a la red interna desde ubicaciones fuera de los campus.
    - Garantiza la seguridad de las conexiones desde cualquier parte del mundo mediante cifrado y autenticación de dos factores.
3. **Redes Segmentadas:**
    - Segmentos de red específicos que están dedicados a diferentes funciones críticas, como redes para la administración de datos financieros, redes para investigación académica, y redes para la gestión de estudiantes.

2. Entornos en la Nube:

1. **Plataformas en la Nube Pública:**
    - Servicios de computación en la nube como Amazon Web Services (AWS), Microsoft Azure, y Google Cloud que UCOP utiliza para el almacenamiento y procesamiento de datos.
    - Estos entornos en la nube manejan tanto aplicaciones de uso general como aplicaciones críticas para la operación administrativa y académica.

2. **Sistemas de Almacenamiento en la Nube:**
    - Almacenamiento de datos en la nube para documentos administrativos, proyectos de investigación, y datos de estudiantes. Los datos están protegidos mediante cifrado y políticas de acceso basadas en roles.

3. **Servicios SaaS (Software as a Service):**
    - Aplicaciones de terceros contratadas para gestionar sistemas académicos, financieros o administrativos que están alojadas en la nube, tales como plataformas de aprendizaje a distancia (LMS) y sistemas de gestión de recursos humanos.

3. Máquinas Virtuales Incluidas:

1. **Servidores Virtuales (VMs):**
    - Máquinas virtuales que ejecutan aplicaciones críticas como bases de datos de estudiantes, sistemas financieros, y software de investigación.
    - Estas VMs están alojadas tanto en servidores locales de UCOP como en entornos de nube híbrida, permitiendo flexibilidad y escalabilidad.
2. **Entornos Virtualizados para Desarrollo y Pruebas:**
    - Entornos virtualizados utilizados para el desarrollo de software interno, pruebas de seguridad, y aplicaciones antes de implementarse en producción.
    - Estos entornos están separados de los sistemas en producción para evitar interferencias y vulnerabilidades.
3. **Máquinas Virtuales para la Continuidad del Negocio:**
    - Máquinas virtuales configuradas específicamente para asegurar la continuidad operativa en caso de un desastre, proporcionando redundancia y respaldos de sistemas críticos.

4. Sistemas y Datos bajo el Control del SGSI:

1. **Sistemas de Gestión de Estudiantes:**
    - Bases de datos y plataformas que contienen información personal de los estudiantes, como calificaciones, historiales académicos, y datos de inscripción.

2. **Sistemas Financieros y Administrativos:**
    - Plataformas y sistemas que manejan la información financiera de la universidad, desde la nómina hasta la gestión presupuestaria.

3. **Sistemas de Investigación:**
    - Bases de datos y servidores que contienen resultados de investigaciones científicas y académicas, así como proyectos en curso que pueden estar sujetos a patentes o derechos de propiedad intelectual.
4. **Datos Sensibles y Privados:**
    - **Datos personales identificables (PII):** Información de empleados, estudiantes, y ciudadanos almacenada en bases de datos que debe ser protegida.
    - **Propiedad intelectual:** Datos de investigación y trabajos académicos que UCOP maneja.

Estos límites virtuales aseguran que todos los entornos de red, plataformas en la nube, y máquinas virtuales que UCOP utiliza para sus operaciones críticas están incluidos dentro del SGSI, con políticas de seguridad específicas aplicadas a cada uno de estos entornos para proteger la integridad y confidencialidad de la información.

Identificación de las Partes Interesadas Clave en el SGSI de UCOP

Basado en la estructura de UCOP y la información disponible en su sitio web (https://security.ucop.edu/index.html), las partes interesadas clave en el Sistema de Gestión de Seguridad de la Información (SGSI) son las siguientes:

1. Equipo de TI

- **Responsabilidades:**
    - Implementar y mantener las políticas de seguridad de la información.
    - Gestionar la infraestructura de TI, como redes, servidores y bases de datos.
    - Monitorear las amenazas y vulnerabilidades en los sistemas de UCOP.
    - Responder a incidentes de seguridad de manera rápida y eficiente.
    - Proporcionar soporte técnico para la implementación de controles de seguridad como firewalls, cifrado y autenticación multifactor.
    - Asegurar la actualización continua del hardware y software, así como aplicar parches de seguridad en sistemas críticos.

2. Gestión Ejecutiva

- **Responsabilidades:**
    - Apoyar y promover el compromiso de la organización con la seguridad de la información.
    - Aprobar y supervisar las políticas de seguridad y los procedimientos asociados.
    - Asignar los recursos financieros y humanos necesarios para implementar y mantener el SGSI.
    - Revisar y aprobar los planes de contingencia y de respuesta a incidentes.
    - Asegurar el cumplimiento de normativas y regulaciones relacionadas con la protección de datos, como la Ley de Privacidad de la Información y otras leyes sectoriales (por ejemplo, HIPAA).

3. Personal Administrativo

- **Responsabilidades:**
    - Aplicar las políticas y procedimientos de seguridad en su gestión diaria.
    - Manejar y proteger información sensible de estudiantes, empleados y pacientes.
    - Reportar cualquier incidente o sospecha de brecha de seguridad de manera oportuna.
    - Cumplir con las políticas de control de acceso, uso adecuado de contraseñas y manejo de datos confidenciales.
    - Participar en las capacitaciones de seguridad de la información ofrecidas por la organización.

4. Estudiantes, Investigadores y Profesores

- **Responsabilidades:**
    - Seguir las políticas de seguridad al acceder a los sistemas de información de la universidad.
    - Proteger sus credenciales de acceso y no compartirlas con terceros.
    - Asegurar que los datos de investigación y académicos estén protegidos, aplicando cifrado y control de acceso cuando sea necesario.
    - Participar en los programas de concienciación y capacitación en seguridad de la información proporcionados por UCOP.

5. Ciudadanos/Pacientes

- **Responsabilidades:**
    - Aunque tienen un papel limitado en la gestión directa de la seguridad, los ciudadanos/pacientes cuyas informaciones son procesadas por UCOP deben estar conscientes de las políticas de privacidad.
    - Reportar cualquier sospecha de mal uso o violación de su información personal a las autoridades correspondientes dentro de la UCOP.

6. Equipo de Cumplimiento y Auditoría

- **Responsabilidades:**
    - Realizar auditorías periódicas del SGSI para evaluar su efectividad y asegurar el cumplimiento con normativas internas y externas.

- Informar a la dirección sobre posibles áreas de mejora y riesgos no mitigados.
- Supervisar el cumplimiento de las regulaciones sectoriales aplicables a la UCOP (como FERPA, HIPAA, y otras).

7. Proveedores y Terceros Externos

- **Responsabilidades:**
  - Cumplir con las políticas de seguridad de UCOP al acceder a los sistemas o manejar información crítica de la organización.
  - Proporcionar los niveles de seguridad adecuados al utilizar plataformas de terceros (como almacenamiento en la nube o soluciones SaaS).
  - Reportar cualquier incidente de seguridad relacionado con los servicios que ofrecen a UCOP.

Asignación de Responsabilidades para las Actividades de Seguridad de la Información

1. **Equipo de TI:** Responsable de la implementación técnica de controles de seguridad, como firewalls, cifrado y autentificación multifactor.
2. **Gestión Ejecutiva:** Responsable de la toma de decisiones estratégicas sobre el SGSI, aprobación de políticas y asignación de recursos.
3. **Personal Administrativo:** Responsable de la protección de datos sensibles y el cumplimiento de políticas de seguridad en el manejo de información.
4. **Estudiantes/Investigadores/Profesores:** Responsables de proteger sus credenciales, seguir las mejores prácticas de seguridad y aplicar controles cuando manejan datos sensibles o académicos.
5. **Equipo de Cumplimiento:** Responsable de monitorear el cumplimiento de las políticas de seguridad y realizar auditorías regulares para evaluar la efectividad del SGSI.
6. **Proveedores Externos:** Responsables de garantizar la seguridad de los servicios que brindan y de seguir las políticas de seguridad de UCOP.

Este enfoque garantiza que todas las partes interesadas clave dentro de UCOP participen activamente en el mantenimiento de la seguridad de la información y cumplan con las responsabilidades que les corresponden según sus roles dentro de la organización.

Documentación del Alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de UCOP

Basado en las características y necesidades descritas en el sitio de UCOP (https://security.ucop.edu/index.html), se presenta la documentación del alcance del SGSI para esta institución.

Propósito del SGSI de UCOP

El Sistema de Gestión de Seguridad de la Información (SGSI) de la **University of California Office of the President (UCOP)** tiene como propósito principal proteger la confidencialidad, integridad y disponibilidad de la información crítica que maneja la universidad. El SGSI busca garantizar que todos los activos de información, tanto físicos como virtuales, sean gestionados de manera segura, minimizando los riesgos de violación de datos, incidentes de seguridad, y asegurando el cumplimiento de normativas regulatorias aplicables, como las leyes estatales y federales sobre privacidad y seguridad de la información (FERPA, HIPAA, entre otras).

Alcance del SGSI

El alcance del SGSI cubre las operaciones relacionadas con la gestión, almacenamiento, transmisión y procesamiento de información crítica para UCOP. Esto incluye:

1. Activos de Información:

- **Datos personales identificables (PII):** Información de estudiantes, empleados y ciudadanos/pacientes.
- **Datos financieros y administrativos:** Información relacionada con la contabilidad, nómina, gestión de presupuestos y otros datos financieros.
- **Datos de investigación:** Propiedad intelectual, estudios científicos y académicos realizados por el personal de UCOP.
- **Infraestructura tecnológica:** Servidores, redes, máquinas virtuales, sistemas en la nube y dispositivos físicos que gestionan los datos críticos de la organización.

2. Áreas Físicas Incluidas:

- Oficinas administrativas de UCOP y sus ubicaciones satélite.
- Centros de datos que almacenan información sensible y operan los sistemas críticos de la universidad.
- Laboratorios de investigación, especialmente aquellos que manejan datos confidenciales o propiedad intelectual.

3. Áreas Virtuales Incluidas:

- Redes internas y segmentadas utilizadas para la transferencia de datos entre diferentes departamentos y campus.
- Entornos de nube pública y privada (por ejemplo, AWS, Azure) utilizados para el almacenamiento y procesamiento de información crítica.
- Máquinas virtuales que soportan los sistemas de información académicos, administrativos y financieros.

Metas del SGSI

1. **Proteger la confidencialidad, integridad y disponibilidad de la información crítica de UCOP.**
2. **Minimizar los riesgos de incidentes de seguridad y violaciones de datos, tanto internas como externas.**
3. **Cumplir con las normativas y regulaciones sectoriales aplicables a la universidad, tales como FERPA, HIPAA y otras leyes estatales y federales.**
4. **Mejorar la concienciación sobre seguridad de la información en todo el personal de la universidad a través de políticas y capacitaciones.**
5. **Establecer un marco de control de acceso riguroso para garantizar que la información solo sea accesible por personas autorizadas.**
6. **Implementar y mantener controles de seguridad robustos, como el cifrado de datos, autenticación multifactor y sistemas de monitoreo continuo.**

Objetivos del SGSI

1. **Mitigar los riesgos relacionados con la ciberseguridad:**
    - Implementar controles específicos para proteger los sistemas contra ciberataques, accesos no autorizados y amenazas internas.
2. **Garantizar la continuidad operativa:**
    - Desarrollar y mantener planes de recuperación ante desastres y asegurar la continuidad del negocio mediante respaldos regulares y redundancias en la infraestructura.

3. **Monitorear y mejorar continuamente:**
    - Establecer métricas de rendimiento de seguridad (KPIs) para evaluar la efectividad de los controles implementados y realizar mejoras de manera proactiva.
4. **Concientización y capacitación:**
    - Asegurar que todos los empleados, desde el equipo administrativo hasta el personal académico, reciban formación regular sobre las políticas y procedimientos de seguridad de la información.

Limitaciones y Exclusiones del SGSI

1. **Exclusión de sistemas no críticos:**
    - Sistemas o plataformas que no manejan información crítica o sensible, como foros de discusión interna o plataformas de mensajería no confidenciales, pueden quedar excluidos del SGSI, ya que su impacto en la seguridad de la organización es limitado.
2. **Exclusión de datos temporales:**
    - Información de carácter temporal o de baja relevancia para las operaciones críticas de la universidad, que no representa un riesgo significativo, puede no estar completamente cubierta por los controles de seguridad más estrictos.
3. **Sistemas de terceros no críticos:**
    - Proveedores externos que no gestionan información crítica o sensible pueden estar excluidos de algunas de las políticas de seguridad más rigurosas, siempre y cuando no manejen datos sensibles.
4. **Información pública:**
    - Datos que ya son públicos o disponibles para el público general no estarán sujetos a los mismos niveles de control que la información confidencial o privada.

Conclusión

El SGSI de UCOP está diseñado para proteger y gestionar de manera segura todos los activos de información críticos de la organización. Con un enfoque centrado en la mitigación de riesgos, el cumplimiento de normativas y la mejora continua, el SGSI abarca todas las áreas clave de seguridad, limitando el alcance únicamente a los sistemas e información que son esenciales para la operación segura y efectiva de la universidad. Las exclusiones identificadas permiten que los recursos se concentren en los activos más críticos, mientras que las políticas de monitoreo y evaluación continua aseguran que el SGSI permanezca adaptable a nuevos desafíos de seguridad.

2.- Evaluación de Riesgos.

Lista de Inventario de Activos para UCOP

Basado en la información disponible en el sitio de UCOP (https://security.ucop.edu/index.html), se desarrolla la siguiente lista de activos, clasificándolos en las categorías de hardware, software, datos y personal, de acuerdo con su importancia dentro del SGSI de UCOP.

1. Hardware

Los dispositivos físicos que forman parte de la infraestructura tecnológica de UCOP.

- **Servidores Físicos:**
    - Servidores dedicados al almacenamiento y procesamiento de información sensible.
    - Clasificación: **Crítico**
- **Computadoras de Escritorio y Portátiles:**
    - Utilizadas por el personal administrativo, estudiantes y profesores para acceder a los sistemas de información.
    - Clasificación: **Alto**
- **Dispositivos de Red (routers, firewalls, switches):**
    - Equipos responsables de la conectividad interna y la seguridad de las redes.
    - Clasificación: **Crítico**
- **Dispositivos de Almacenamiento:**
    - Unidades NAS (almacenamiento en red) y discos duros externos utilizados para copias de seguridad y almacenamiento temporal de datos.
    - Clasificación: **Alto**
- **Equipos de Laboratorio:**
    - Dispositivos especializados utilizados en investigaciones académicas y proyectos científicos.
    - Clasificación: **Medio**

2. Software

Sistemas operativos, aplicaciones y plataformas que gestionan los datos y operaciones dentro de UCOP.

- **Sistemas Operativos (Windows, Linux, macOS):**
    - Instalados en servidores y computadoras para gestionar el acceso a la red y las aplicaciones.
    - Clasificación: **Crítico**
- **Sistemas de Gestión Académica (PeopleSoft, plataformas LMS):**
    - Aplicaciones que gestionan la información de los estudiantes y procesos académicos.
    - Clasificación: **Crítico**
- **Sistemas de Gestión Financiera y Administrativa:**
    - Aplicaciones que manejan la contabilidad, nómina y otros aspectos financieros.
    - Clasificación: **Crítico**
- **Aplicaciones de Investigación:**
    - Software especializado utilizado por los investigadores para proyectos científicos y académicos.
    - Clasificación: **Alto**
- **Sistemas de Almacenamiento en la Nube (AWS, Google Cloud, Microsoft Azure):**
    - Plataformas en la nube donde se almacenan y procesan datos sensibles y archivos críticos.
    - Clasificación: **Alto**

3. Datos

La información crítica que UCOP maneja en sus diferentes áreas, incluyendo académica, administrativa y de investigación.

- **Datos de Estudiantes (PII):**
    - Información personal identificable de estudiantes, que incluye nombres, direcciones, calificaciones, historiales académicos y financieros.
    - Clasificación: **Crítico**

- **Datos de Empleados (PII):**
    - Información de los empleados que incluye nómina, datos personales y registros laborales.
    - Clasificación: **Crítico**
- **Datos Financieros:**
    - Información sobre la contabilidad, presupuesto, pagos y otros aspectos financieros de la universidad.
    - Clasificación: **Crítico**
- **Datos de Investigación:**
    - Información relacionada con proyectos de investigación, incluyendo propiedad intelectual y datos experimentales.
    - Clasificación: **Crítico**
- **Registros Administrativos:**
    - Datos sobre las operaciones diarias de la universidad que incluyen registros de recursos humanos y operaciones internas.
    - Clasificación: **Alto**

4. Personal

Los individuos que interactúan con los sistemas y activos de UCOP, y cuya participación es fundamental para la protección de los activos.

- **Equipo de TI:**
    - Personal responsable de la gestión de infraestructura, redes y sistemas de seguridad.
    - Clasificación: **Crítico**
- **Administradores de Sistemas:**
    - Encargados de gestionar los servidores, redes y plataformas críticas.
    - Clasificación: **Crítico**
- **Académicos e Investigadores:**
    - Personal involucrado en la creación y gestión de datos de investigación y proyectos académicos.
    - Clasificación: **Alto**

- **Personal Administrativo:**
    - Personal encargado de manejar datos financieros, administrativos y de estudiantes.
    - Clasificación: **Alto**
- **Estudiantes:**
    - Usuarios que interactúan con los sistemas académicos y las plataformas de aprendizaje.
    - Clasificación: **Medio**

Resumen Clasificación de Activos

- **Crítico:** Servidores físicos, sistemas operativos, sistemas de gestión académica y financiera, datos de estudiantes y empleados, equipo de TI y administradores de sistemas.
- **Alto:** Computadoras personales, dispositivos de red, sistemas en la nube, datos financieros, personal administrativo, académicos e investigadores.
- **Medio:** Equipos de laboratorio, aplicaciones de investigación, estudiantes.

Este inventario y clasificación permiten entender la criticidad de cada activo dentro del SGSI y proporcionan una base sólida para priorizar controles de seguridad y recursos para mitigar riesgos asociados a estos activos.

Identificación de Amenazas Potenciales para UCOP

Basado en la página de UCOP (https://security.ucop.edu/index.html), a continuación se describen las amenazas potenciales que podrían afectar los activos clave dentro del Sistema de Gestión de Seguridad de la Información (SGSI) de UCOP.

Amenazas Externas:

1. **Acceso no autorizado (intrusiones externas):**
    - **Descripción:** Hackers o actores maliciosos externos intentan acceder a los sistemas de UCOP, ya sea a través de la explotación de vulnerabilidades en la red, software o mediante credenciales robadas.

- **Activos afectados:**
    - **Sistemas financieros.**
    - **Datos personales (PII) de estudiantes y empleados.**
    - **Plataformas en la nube.**

2. **Malware, Ransomware y Phishing:**
    - **Descripción:** Ataques cibernéticos diseñados para interrumpir el servicio, comprometer la información sensible o extorsionar a la organización bloqueando los datos.
    - **Activos afectados:**
        - **Sistemas operativos y bases de datos.**
        - **Aplicaciones críticas, incluidas las plataformas de gestión académica y financiera.**
        - **Dispositivos de red.**
3. **Violación de datos personales:**
    - **Descripción:** Los datos sensibles (PII, información financiera) de estudiantes, empleados o pacientes pueden ser expuestos debido a ciberataques o errores humanos, lo que podría llevar a pérdidas financieras y problemas legales.
    - **Activos afectados:**
        - **Bases de datos de estudiantes, empleados y ciudadanos.**
        - **Sistemas de almacenamiento en la nube.**
4. **Desastres naturales (terremotos, incendios, inundaciones):**
    - **Descripción:** Eventos naturales que pueden dañar la infraestructura física de UCOP, incluidos los centros de datos, lo que lleva a una pérdida de datos y la interrupción de servicios críticos.
    - **Activos afectados:**
        - **Centros de datos y dispositivos de almacenamiento.**
        - **Servidores físicos y dispositivos de respaldo.**

5. **Interrupciones en la infraestructura tecnológica:**
    - **Descripción:** Fallos en los sistemas de red o infraestructura, como caídas de servidores, fallas de energía o interrupciones en la conectividad.
    - **Activos afectados:**
        - **Sistemas de red interna.**
        - **Servidores y sistemas críticos de la universidad.**

<u>Amenazas Internas:</u>

1. **Errores humanos:**
    - **Descripción:** Los empleados o usuarios internos pueden cometer errores involuntarios que resulten en la exposición de información crítica, ya sea al compartir datos sensibles o realizar configuraciones incorrectas.
    - **Activos afectados:**
        - **Datos personales (PII).**
        - **Sistemas financieros.**
        - **Sistemas de gestión académica.**
2. **Acceso malintencionado por empleados internos:**
    - **Descripción:** Empleados o personal con acceso privilegiado podrían utilizar sus credenciales para obtener información confidencial con fines maliciosos, como el robo de datos o el espionaje.
    - **Activos afectados:**
        - **Bases de datos sensibles.**
        - **Sistemas financieros y académicos.**
3. **Falta de actualización y mantenimiento de sistemas:**
    - **Descripción:** Si los sistemas y software no se mantienen actualizados, se exponen a vulnerabilidades que pueden ser explotadas por actores malintencionados, tanto internos como externos.
    - **Activos afectados:**
        - **Sistemas operativos.**
        - **Aplicaciones críticas y plataformas en la nube.**

4. **Manejo inadecuado de contraseñas:**
    - **Descripción:** La falta de políticas estrictas de contraseñas (contraseñas débiles o reutilizadas) podría permitir que los atacantes accedan a sistemas críticos de manera no autorizada.
    - **Activos afectados:**
        - **Sistemas financieros y académicos.**
        - **Redes y plataformas de almacenamiento.**
5. **Fallas en la implementación de controles de seguridad:**
    - **Descripción:** Si los controles de seguridad (como el cifrado o la autenticación multifactor) no se implementan adecuadamente, los sistemas pueden quedar expuestos a ataques internos o externos.
    - **Activos afectados:**
        - **Datos personales (PII).**
        - **Aplicaciones en la nube y sistemas críticos.**

Resumen de Amenazas por Tipo de Activo

1. **Sistemas financieros y académicos:**
    - **Amenazas externas:** Acceso no autorizado, malware, violación de datos.
    - **Amenazas internas:** Errores humanos, manejo inadecuado de contraseñas, acceso malintencionado.
2. **Datos personales (PII):**
    - **Amenazas externas:** Violaciones de datos, ransomware, intrusiones.
    - **Amenazas internas:** Errores humanos, falta de controles de acceso, uso indebido de acceso privilegiado.
3. **Centros de datos y servidores:**
    - **Amenazas externas:** Desastres naturales, interrupciones de infraestructura, malware.
    - **Amenazas internas:** Falta de mantenimiento, errores humanos.

4. **Plataformas en la nube y almacenamiento:**
    - **Amenazas externas:** Acceso no autorizado, violaciones de datos, fallas de red.
    - **Amenazas internas:** Acceso malintencionado, contraseñas débiles, fallas de implementación de seguridad.

Esta identificación de amenazas proporciona una base sólida para continuar con la evaluación de riesgos y la implementación de controles específicos dentro del SGSI de UCOP.

Identificación de Vulnerabilidades en UCOP

Basado en la información disponible en el sitio de UCOP (https://security.ucop.edu/index.html), a continuación se describen las vulnerabilidades que podrían exponer los activos críticos a las amenazas identificadas en el Sistema de Gestión de Seguridad de la Información (SGSI).

Vulnerabilidades Técnicas

1. **Falta de cifrado de datos sensibles (en reposo y en tránsito):**
    - **Descripción:** Si los datos personales (PII), financieros y de investigación no están cifrados adecuadamente, pueden ser interceptados por actores malintencionados tanto dentro de la red interna como durante la transmisión entre servidores o plataformas en la nube.
    - **Explotación:** Los hackers podrían interceptar comunicaciones no cifradas o acceder a datos almacenados en sistemas comprometidos, resultando en una violación de datos.
    - **Activos afectados:**
        - **Bases de datos de estudiantes y empleados.**
        - **Sistemas financieros.**
        - **Sistemas de investigación.**
2. **Contraseñas débiles o políticas de gestión de contraseñas deficientes:**
    - **Descripción:** El uso de contraseñas débiles o la falta de una política que obligue a cambiar las contraseñas regularmente expone los sistemas a

ataques de fuerza bruta, donde los atacantes intentan acceder usando múltiples combinaciones de contraseñas.

- **Explotación:** Los atacantes pueden usar ataques de diccionario o fuerza bruta para obtener acceso a cuentas de usuarios y sistemas críticos, comprometiendo información sensible.
- **Activos afectados:**
  - **Sistemas de gestión académica y financiera.**
  - **Plataformas de almacenamiento en la nube.**
  - **Sistemas operativos y aplicaciones críticas.**

3. **Sistemas desactualizados (falta de parches de seguridad):**
   - **Descripción:** Los sistemas operativos, aplicaciones y servidores que no reciben actualizaciones o parches de seguridad periódicos son vulnerables a exploits conocidos y malware.
   - **Explotación:** Los atacantes pueden aprovechar vulnerabilidades ya conocidas para lanzar ataques automatizados o específicos contra sistemas desactualizados.
   - **Activos afectados:**
     - **Servidores.**
     - **Redes internas.**
     - **Plataformas de gestión académica y aplicaciones SaaS.**
4. **Fallas en la configuración de los controles de acceso:**
   - **Descripción:** Si los permisos y controles de acceso no están configurados adecuadamente, usuarios no autorizados podrían acceder a información confidencial o a sistemas que no necesitan para su trabajo.
   - **Explotación:** Los atacantes o empleados internos malintencionados podrían explotar permisos mal configurados para obtener acceso a datos confidenciales o sistemas críticos.
   - **Activos afectados:**
     - **Bases de datos sensibles.**
     - **Sistemas financieros.**
     - **Redes internas.**

5. **Falta de autenticación multifactor (MFA):**
    - **Descripción:** La ausencia de autenticación multifactor (MFA) deja a los sistemas vulnerables al acceso mediante credenciales robadas, ya que la única barrera para acceder son las contraseñas.
    - **Explotación:** Si un atacante obtiene acceso a las credenciales de un usuario, puede acceder a sistemas críticos sin necesidad de una segunda capa de autenticación.
    - **Activos afectados:**
        - **Sistemas financieros y de recursos humanos.**
        - **Plataformas en la nube.**
        - **Sistemas académicos y administrativos.**
6. **Falta de monitoreo y respuesta a incidentes:**
    - **Descripción:** Si no se implementan soluciones de monitoreo continuo para detectar incidentes de seguridad o actividad sospechosa en la red, los ataques pueden pasar desapercibidos durante largos periodos.
    - **Explotación:** Los atacantes pueden explotar la falta de visibilidad y realizar movimientos laterales dentro de la red o acceder a múltiples sistemas sin ser detectados.
    - **Activos afectados:**
        - **Redes internas.**
        - **Sistemas operativos y aplicaciones.**
        - **Sistemas de almacenamiento en la nube.**

Vulnerabilidades Organizacionales

1. **Capacitación insuficiente en seguridad de la información:**
    - **Descripción:** Si los empleados no reciben una formación adecuada en las mejores prácticas de seguridad, pueden caer en ataques de ingeniería social, como el phishing, o no seguir los procedimientos de seguridad correctamente.
    - **Explotación:** Los atacantes pueden aprovecharse de la falta de conocimiento del personal para obtener información sensible a través de engaños o errores humanos.

- **Activos afectados:**
    - **Datos personales (PII).**
    - **Sistemas financieros y académicos.**
    - **Plataformas de almacenamiento en la nube.**

2. **Falta de políticas robustas de gestión de incidentes:**
    - **Descripción:** La falta de procedimientos claramente definidos para la respuesta a incidentes de seguridad podría retrasar la contención y mitigación de un ataque, aumentando el impacto.
    - **Explotación:** Los atacantes pueden aprovechar el tiempo de reacción lento de la organización para extender su control sobre más sistemas o datos.
    - **Activos afectados:**
        - **Sistemas críticos y bases de datos.**
        - **Redes internas.**
        - **Aplicaciones en la nube.**
3. **Dependencia de proveedores externos sin suficiente control de seguridad:**
    - **Descripción:** Los proveedores externos que no cumplen con los mismos estándares de seguridad pueden introducir vulnerabilidades en el entorno de UCOP, especialmente si no se evalúan adecuadamente los riesgos.
    - **Explotación:** Los atacantes pueden explotar vulnerabilidades en los sistemas de los proveedores para comprometer la información de UCOP.
    - **Activos afectados:**
        - **Plataformas SaaS (Software as a Service).**
        - **Sistemas de almacenamiento en la nube.**

Evaluación de cómo pueden ser explotadas las vulnerabilidades

1. **Cifrado insuficiente:** Los datos sensibles en tránsito o en reposo pueden ser interceptados y leídos por atacantes si no están cifrados adecuadamente, exponiendo información crítica y confidencial.

2. **Contraseñas débiles:** Los ataques de fuerza bruta pueden aprovecharse de contraseñas simples o reutilizadas, lo que permite a los atacantes obtener acceso no autorizado.
3. **Sistemas desactualizados:** Los atacantes pueden utilizar herramientas automáticas para escanear y atacar sistemas con vulnerabilidades conocidas que no han sido parcheadas.
4. **Permisos mal configurados:** Los usuarios con acceso excesivo o mal configurado pueden realizar acciones no autorizadas, como acceder o modificar datos críticos.
5. **Falta de autenticación multifactor:** Los atacantes que obtienen credenciales pueden acceder a sistemas críticos sin ser detenidos por un segundo factor de autenticación, lo que facilita violaciones de seguridad.
6. **Falta de monitoreo:** Un ataque prolongado podría pasar desapercibido sin la implementación de herramientas de monitoreo continuo, lo que permite que el atacante mantenga el acceso durante periodos extendidos sin ser detectado.

Conclusión

Estas vulnerabilidades representan puntos clave donde UCOP podría estar expuesta a diversas amenazas. Es crucial priorizar la mitigación de estas vulnerabilidades mediante la implementación de controles como el cifrado, la autenticación multifactor y el monitoreo constante, además de reforzar las políticas de gestión de incidentes y la capacitación del personal.

Priorización de Riesgos en UCOP

La priorización de riesgos se basa en la **probabilidad** de ocurrencia y el **impacto** potencial en la organización si estos riesgos se materializan. Esto permite asignar una calificación de riesgo a cada amenaza identificada y priorizar las que requieren atención o mitigación inmediata para proteger los activos de UCOP.

---

1. Asignación de Calificación de Riesgo

Riesgo Identificado	Probabilidad	Impacto	Calificación de Riesgo
Ciberataques (malware, ransomware)	Alta	Alto	Muy Alto
Acceso no autorizado	Media	Alto	Alto
Violaciones de datos personales	Alta	Muy Alto	Muy Alto
Errores humanos	Alta	Medio	Medio
Empleados malintencionados	Media	Alto	Alto
Sistemas desactualizados	Alta	Medio	Alto
Falta de cifrado	Media	Muy Alto	Muy Alto
Desastres naturales	Baja	Alto	Medio
Interrupciones en la infraestructura	Media	Alto	Alto
Falta de autenticación multifactor (MFA)	Alta	Alto	Muy Alto
Falta de monitoreo y respuesta a incidentes	Media	Alto	Alto

---

2. Priorización de Riesgos para Mitigación Inmediata

Para la priorización, los riesgos de **Muy Alto** requieren atención y mitigación inmediata debido a su impacto crítico en la organización. Estos riesgos pueden causar compromisos graves de la seguridad de los activos y afectar la continuidad operativa y la confidencialidad de los datos.

Riesgos con Prioridad de Mitigación Inmediata (Calificación Muy Alto):

1. **Ciberataques (malware, ransomware):**
    - **Descripción:** La alta probabilidad y el impacto crítico hacen que este riesgo sea una prioridad, especialmente debido a la posibilidad de pérdida de datos y extorsión financiera.
    - **Medidas de mitigación:** Implementar sistemas de detección de intrusos, firewalls de última generación, y políticas de backup y restauración de datos.
2. **Violaciones de datos personales:**
    - **Descripción:** Debido a la naturaleza sensible de los datos personales, una violación de estos datos puede resultar en sanciones legales y dañar la reputación de UCOP.
    - **Medidas de mitigación:** Implementar cifrado de datos, controles de acceso estrictos y monitoreo continuo.
3. **Falta de cifrado de datos sensibles:**
    - **Descripción:** La ausencia de cifrado para datos críticos aumenta la vulnerabilidad a accesos no autorizados y exposición de datos en caso de ataques.
    - **Medidas de mitigación:** Establecer el cifrado obligatorio para datos en reposo y en tránsito, y revisar las políticas de cifrado regularmente.
4. **Falta de autenticación multifactor (MFA):**
    - **Descripción:** La falta de MFA incrementa el riesgo de accesos no autorizados mediante el uso de credenciales comprometidas.
    - **Medidas de mitigación:** Implementar MFA en todos los sistemas críticos y para todas las cuentas de acceso privilegiado.

Riesgos con Alta Prioridad (Calificación Alto):

1. **Acceso no autorizado:**
    - **Medidas de mitigación:** Implementar controles de acceso basado en roles (RBAC), auditorías regulares de permisos y revisar configuraciones de seguridad en servidores y redes.

2. **Empleados malintencionados:**
    - **Medidas de mitigación:** Monitorear actividades anómalas, establecer controles internos de acceso, y realizar capacitaciones de seguridad para el personal.
3. **Sistemas desactualizados:**
    - **Medidas de mitigación:** Implementar un sistema de gestión de parches, programar actualizaciones de software regularmente y utilizar herramientas de monitoreo para verificar la actualización de sistemas.
4. **Interrupciones en la infraestructura:**
    - **Medidas de mitigación:** Implementar redundancias y sistemas de respaldo para datos críticos y establecer políticas de recuperación ante desastres.
5. **Falta de monitoreo y respuesta a incidentes:**
    - **Medidas de mitigación:** Implementar herramientas de monitoreo en tiempo real, definir procedimientos claros de respuesta a incidentes y capacitar al personal en su detección y respuesta.

Conclusión

Para UCOP, los riesgos de "Muy Alto" son los primeros en requerir mitigación debido a su impacto potencialmente devastador en la seguridad de la información y la operatividad de la institución. Se debe implementar un enfoque proactivo para reducir estos riesgos, centrándose en controles técnicos como el cifrado, MFA, monitoreo, y el endurecimiento de sistemas contra ciberataques y accesos no autorizados. Los riesgos con prioridad "Alto" también deben ser gestionados, con planes de acción que incluyan controles de acceso, gestión de parches y formación en seguridad para el personal.

4.- Selección de Controles.

Selección de Controles de Seguridad para UCOP

Basado en los riesgos prioritarios identificados y la información disponible en la página de UCOP (https://security.ucop.edu/index.html), se eligen los controles de seguridad más efectivos para mitigar los riesgos y proteger los activos de UCOP. Estos controles se basan en estándares como **ISO/IEC 27001**, **NIST** y prácticas recomendadas para asegurar la confidencialidad, integridad y disponibilidad de la información.

Controles de Seguridad Seleccionados

1. Ciberataques (Malware, Ransomware)

- **Firewall de Próxima Generación (NGFW):**
    - Controla el tráfico de red y protege contra ataques externos mediante inspección avanzada y filtrado de contenido.
- **Sistemas de Detección y Prevención de Intrusos (IDPS):**
    - Detecta y previene ataques a la red de UCOP, alertando sobre actividades sospechosas en tiempo real.
- **Antivirus y Antimalware Actualizados:**
    - Asegura que todos los sistemas, incluyendo servidores y estaciones de trabajo, estén protegidos contra malware.
- **Respaldo y Recuperación de Datos:**
    - Implementa copias de seguridad regulares para garantizar la recuperación en caso de un ataque de ransomware.

2. Violaciones de Datos Personales

- **Cifrado de Datos Sensibles en Reposo y en Tránsito:**
    - Aplica cifrado en bases de datos y para toda la información transmitida entre sistemas, protegiendo datos personales de estudiantes y empleados.
- **Control de Acceso Basado en Roles (RBAC):**
    - Limita el acceso a datos personales solo al personal autorizado, asegurando que los usuarios solo accedan a la información necesaria para sus roles.
- **Política de Retención de Datos:**

- Define períodos específicos para la retención y eliminación de datos personales, minimizando la exposición de datos innecesarios.

3. Falta de Cifrado de Datos Sensibles

- **Cifrado Obligatorio para Datos Críticos:**
  - Implementa soluciones de cifrado en todos los sistemas que manejen datos críticos, como sistemas financieros y de investigación.
- **Gestión de Claves de Cifrado Segura:**
  - Asegura que las claves de cifrado estén protegidas y gestionadas adecuadamente, con un acceso restringido solo al personal autorizado.
- **Revisión y Monitoreo de Configuración de Cifrado:**
  - Monitorea regularmente la configuración de cifrado para detectar y corregir cualquier vulnerabilidad o configuración incorrecta.

4. Falta de Autenticación Multifactor (MFA)

- **Implementación de Autenticación Multifactor (MFA) en Sistemas Críticos:**
  - Aplica MFA en los sistemas de mayor importancia, como sistemas financieros, aplicaciones de recursos humanos y plataformas en la nube, para proteger contra accesos no autorizados.
- **Políticas de Contraseñas Seguras:**
  - Establece requisitos de contraseñas fuertes (longitud mínima, complejidad) y rotación de contraseñas periódica.
- **Capacitación en Seguridad para la Gestión de Credenciales:**
  - Educa al personal sobre la importancia de MFA y de la protección de sus credenciales de acceso.

5. Acceso No Autorizado

- **Política de Control de Acceso Basado en Privilegios Mínimos:**
  - Limita el acceso a sistemas críticos solo a personal esencial, aplicando el principio de privilegio mínimo.
- **Auditorías Regulares de Acceso:**
  - Revisa los permisos de acceso periódicamente y retira el acceso a los usuarios que ya no lo necesitan.
- **Registro y Monitoreo de Actividades de Usuarios:**

- Implementa un sistema de registro de auditoría para rastrear el acceso y las actividades dentro de los sistemas críticos, permitiendo detectar posibles accesos no autorizados.

6. Empleados Malintencionados

- **Sistemas de Monitoreo y Detección de Actividades Anómalas:**
  - Monitorea el comportamiento de usuarios en busca de actividades sospechosas o desviaciones en el uso de datos críticos.
- **Segregación de Funciones y Restricciones en el Acceso:**
  - Divide y limita las responsabilidades en la gestión de datos críticos para reducir la posibilidad de abuso de acceso.
- **Capacitación Regular en Seguridad y Ética:**
  - Realiza capacitaciones de concienciación en seguridad para empleados, destacando las políticas de seguridad y las consecuencias del mal uso de los datos.

7. Sistemas Desactualizados

- **Política de Gestión de Parches y Actualizaciones:**
  - Establece un sistema de gestión para aplicar actualizaciones y parches de seguridad periódicos en todos los sistemas críticos.
- **Inventario de Software y Verificación de Versiones:**
  - Mantiene un inventario actualizado de todo el software utilizado en UCOP y revisa regularmente su estado de actualización.
- **Pruebas de Compatibilidad y Validación de Parches:**
  - Antes de la implementación, realiza pruebas para garantizar que los parches de seguridad no afecten la funcionalidad de los sistemas.

8. Interrupciones en la Infraestructura

- **Planes de Continuidad de Negocio y Recuperación ante Desastres (BCP/DRP):**
  - Desarrolla y prueba regularmente los planes de continuidad y recuperación para asegurar la operación en caso de fallos o desastres.
- **Redundancia de Infraestructura Crítica:**
  - Implementa redundancias (servidores, almacenamiento) para asegurar que los sistemas críticos permanezcan operativos.

- **Respaldo de Energía y Conexión Alternativa:**
    - Asegura la disponibilidad de energía y conectividad de respaldo para mitigar interrupciones.

9. Falta de Monitoreo y Respuesta a Incidentes

- **Implementación de un Centro de Operaciones de Seguridad (SOC):**
    - Centraliza el monitoreo de amenazas y gestión de incidentes en un SOC dedicado, con un equipo disponible 24/7.
- **Sistemas de Gestión de Eventos e Información de Seguridad (SIEM):**
    - Recopila y analiza datos de registros en tiempo real para detectar posibles amenazas y responder de inmediato.
- **Plan de Respuesta a Incidentes (IRP):**
    - Define procedimientos detallados para la detección, respuesta y recuperación ante incidentes, asignando responsabilidades claras al personal de TI.

Conclusión

Los controles seleccionados buscan abordar los riesgos prioritarios de UCOP mediante una combinación de medidas técnicas y organizacionales, asegurando la seguridad integral de los activos críticos de la institución. Estos controles no solo mitigan los riesgos de ciberataques y accesos no autorizados, sino que también fortalecen la cultura de seguridad dentro de UCOP y aseguran la continuidad operativa en situaciones críticas.

Revisión de Normas Relevantes para el SGSI de UCOP

Para establecer un SGSI eficaz en UCOP y mitigar los riesgos identificados, se revisan las normas de seguridad de la información **ISO/IEC 27001**, **NIST (National Institute of Standards and Technology)** y **CIS (Center for Internet Security)**, así como regulaciones específicas como **HIPAA** para el manejo de información de salud. Estas normas proporcionan directrices y controles específicos para la gestión y protección de la información.

1. ISO/IEC 27001

La norma **ISO/IEC 27001** es un estándar internacional para la gestión de la seguridad de la información, y proporciona un marco para establecer, implementar, mantener y mejorar continuamente un SGSI. Algunos controles relevantes de la norma ISO/IEC 27001 que aplican para UCOP incluyen:

- **A.9 Control de Acceso:**
    - Control de acceso basado en roles (RBAC) y autenticación multifactor (MFA) para proteger el acceso a sistemas críticos y datos sensibles.
- **A.10 Cifrado:**
    - Requerimiento de cifrado para datos sensibles en reposo y en tránsito, aplicable a datos personales y de investigación en UCOP.
- **A.12 Seguridad en las Operaciones:**
    - Implementación de controles para la gestión de parches, monitoreo de seguridad, y gestión de eventos de seguridad (SIEM) para detectar y responder a amenazas en tiempo real.
- **A.16 Gestión de Incidentes de Seguridad de la Información:**
    - Desarrollo de un Plan de Respuesta a Incidentes (IRP), con un procedimiento formal de reporte y gestión de incidentes para contener y remediar amenazas.

Aplicabilidad:

La ISO/IEC 27001 es altamente aplicable para los riesgos de UCOP, especialmente en la gestión de accesos, cifrado de datos y respuesta a incidentes, y cumple con las expectativas regulatorias de confidencialidad, integridad y disponibilidad de datos.

2. NIST (National Institute of Standards and Technology)

El **NIST Cybersecurity Framework** (CSF) es un marco de referencia común en Estados Unidos, utilizado para gestionar y reducir el riesgo cibernético mediante cinco funciones principales: **Identificar**, **Proteger**, **Detectar**, **Responder** y **Recuperar**. Controles NIST relevantes para UCOP incluyen:

- **Access Control (AC-2):**
    - Revisión periódica de los privilegios de acceso y configuración de acceso basado en roles y privilegios mínimos, cubriendo riesgos de acceso no autorizado.
- **Risk Assessment (RA-5):**
    - Identificación y evaluación continua de vulnerabilidades para gestionar el riesgo en sistemas desactualizados y fallas de configuración.
- **System and Information Integrity (SI-4):**
    - Monitoreo continuo de eventos de seguridad para identificar y responder rápidamente a incidentes.
- **Incident Response (IR-4):**
    - Desarrollo de un plan de respuesta y recuperación ante incidentes, con un equipo designado y roles claramente definidos.

Aplicabilidad:

El NIST CSF es adecuado para gestionar la infraestructura de UCOP, especialmente en la supervisión de incidentes, control de accesos y análisis de vulnerabilidades. Este marco es compatible con normas sectoriales como **FERPA** y **HIPAA**, cumpliendo los requisitos de privacidad y protección de datos para UCOP.

3. CIS (Center for Internet Security)

Las recomendaciones de **CIS Controls** proporcionan controles específicos y prácticos que UCOP puede implementar para fortalecer su ciberseguridad. Algunos controles relevantes incluyen:

- **Control 1: Inventario y Control de Activos de Hardware:**
    - Mantenimiento de un inventario completo de hardware para asegurar que todos los dispositivos se mantengan actualizados y supervisados.
- **Control 4: Control de Privilegios Administrativos:**

    - Implementación de políticas de acceso basado en privilegios mínimos y auditorías de acceso para mitigar el riesgo de usuarios malintencionados.

- **Control 7: Protección Contra Malware:**
    - Implementación de herramientas antimalware en todos los sistemas críticos para mitigar amenazas como malware y ransomware.
- **Control 10: Configuración Segura de Dispositivos de Red:**
    - Configuración segura de routers, switches y firewalls para proteger la red interna de UCOP de accesos externos no autorizados.

Aplicabilidad:

Los controles de CIS son adecuados para mitigar riesgos operacionales específicos en UCOP, como el control de acceso, administración de activos y protección contra malware, mejorando la resiliencia frente a ciberataques y amenazas internas.

4. Regulaciones Específicas: HIPAA

La **Health Insurance Portability and Accountability Act (HIPAA)** es relevante para UCOP, especialmente en el manejo de datos de salud de estudiantes o empleados. HIPAA requiere controles específicos para garantizar la privacidad y seguridad de la información de salud. Controles relevantes incluyen:

- **Security Rule - Administrative Safeguards:**
    - Controles administrativos como el monitoreo de acceso y la implementación de un plan de respuesta a incidentes para proteger la información de salud.
- **Security Rule - Technical Safeguards:**
    - Cifrado y control de acceso para asegurar que los datos de salud estén protegidos tanto en reposo como en tránsito.
- **Privacy Rule:**
    - Establece requisitos de privacidad para garantizar que la información de salud esté protegida y que solo el personal autorizado pueda acceder a estos datos.

Aplicabilidad:

HIPAA es esencial para el cumplimiento normativo en el sector salud de UCOP, especialmente en el tratamiento de datos de pacientes y estudiantes, donde el cifrado, control de acceso y gestión de incidentes juegan un papel fundamental.

Resumen de Controles Relevantes

Norma	Control Relevante	Aplicación en UCOP
ISO/IEC 27001	Cifrado, Control de Acceso, Gestión de Incidentes	Protege datos personales, controla accesos y formaliza la respuesta a incidentes.
NIST CSF	Control de Acceso, Monitoreo, Respuesta a Incidentes	Fortalece la protección de la red, asegura la respuesta ante incidentes y mitiga riesgos de acceso.
CIS Controls	Inventario, Protección Antimalware, Configuración Segura	Garantiza la actualización de dispositivos, la protección contra malware y la configuración de red segura.
HIPAA	Seguridad y Privacidad en Datos de Salud	Protege la información de salud mediante cifrado y control de acceso, cumpliendo con requisitos regulatorios.

Las normas y controles seleccionados permiten a UCOP mitigar de manera eficaz los riesgos identificados, cumpliendo además con regulaciones específicas del sector, como HIPAA para datos de salud y FERPA para datos académicos. Este marco de controles garantiza un enfoque integral en la gestión de la seguridad, la confidencialidad y la integridad de la información crítica de UCOP.

Selección de Controles de Seguridad para UCOP

Basado en la información de https://security.ucop.edu/index.html y considerando los riesgos prioritarios identificados para UCOP, a continuación se seleccionan los controles de seguridad más adecuados para mitigar estos riesgos. Se eligen controles específicos y efectivos que, además de abordar las amenazas clave, sean factibles y sostenibles dentro del entorno del sector público.

Controles de Seguridad Seleccionados

1. Firewalls de Próxima Generación (NGFW)

- **Descripción:** Los NGFW inspeccionan todo el tráfico de red en busca de amenazas avanzadas, aplicando filtros de contenido y control de aplicaciones para prevenir accesos no autorizados y ataques externos.
- **Aplicación en UCOP:**
    - Implementación de firewalls en los perímetros de red y en las ubicaciones críticas de la infraestructura.
- **Factibilidad:** Los NGFW pueden ser gestionados internamente por el equipo de TI de UCOP y pueden ser escalados según las necesidades de tráfico de la organización.

2. Autenticación Multifactor (MFA)

- **Descripción:** MFA proporciona una capa adicional de seguridad al requerir más de un método de autenticación, lo que mitiga el riesgo de accesos no autorizados mediante credenciales comprometidas.
- **Aplicación en UCOP:**
    - Implementar MFA para sistemas críticos como sistemas financieros, recursos humanos y aplicaciones en la nube.
- **Factibilidad:** Existen soluciones de MFA que son accesibles y compatibles con aplicaciones públicas, y pueden ser implementadas en sistemas clave de forma gradual según los recursos disponibles.

3. Cifrado de Datos Sensibles (en reposo y en tránsito)

- **Descripción:** El cifrado asegura que los datos, tanto en almacenamiento como durante la transmisión, estén protegidos contra accesos no autorizados o intercepciones.

- **Aplicación en UCOP:**
    - Cifrado en bases de datos de estudiantes, empleados y en la información financiera y de investigación.
- **Factibilidad:** Las soluciones de cifrado para datos en reposo y en tránsito están disponibles en aplicaciones de bases de datos y almacenamiento en la nube, permitiendo a UCOP implementar esta medida en fases, comenzando con los datos de mayor riesgo.

4. Control de Acceso Basado en Roles (RBAC)

- **Descripción:** RBAC permite asignar permisos específicos a los usuarios según sus funciones, limitando el acceso a la información y reduciendo el riesgo de accesos indebidos.
- **Aplicación en UCOP:**
    - Establecer permisos de acceso para que solo el personal necesario tenga acceso a datos críticos y sistemas administrativos.
- **Factibilidad:** RBAC puede integrarse en los sistemas actuales de UCOP con soporte del equipo de TI, y se ajusta fácilmente a las necesidades operativas de una organización pública con una estructura jerárquica.

5. Sistemas de Detección y Prevención de Intrusos (IDPS)

- **Descripción:** IDPS monitorea la actividad de la red en tiempo real para identificar y detener amenazas antes de que afecten los sistemas.
- **Aplicación en UCOP:**
    - Implementación de IDPS en la red interna y perimetral para detectar patrones de comportamiento anómalo y detener posibles ataques.
- **Factibilidad:** Las soluciones IDPS se pueden adaptar a la infraestructura existente y se pueden implementar con opciones de administración local o en la nube, lo cual es compatible con los recursos de UCOP.

6. Gestión de Parches y Actualizaciones

- **Descripción:** La gestión de parches permite aplicar actualizaciones de seguridad en los sistemas operativos y software, mitigando vulnerabilidades conocidas.
- **Aplicación en UCOP:**
    - Establecer un calendario regular de parches para sistemas operativos, aplicaciones críticas y dispositivos de red.

- **Factibilidad:** Los recursos de TI de UCOP pueden programar parches de manera regular, priorizando los sistemas críticos, lo cual es viable dentro del presupuesto y los recursos técnicos actuales.

7. Respaldo y Recuperación de Datos

- **Descripción:** La realización de copias de seguridad frecuentes y el establecimiento de un plan de recuperación aseguran que los datos puedan recuperarse en caso de un ataque o desastre.
- **Aplicación en UCOP:**
    - Copias de seguridad diarias de sistemas críticos, como datos de estudiantes, financieros y de investigación, y pruebas trimestrales de recuperación.
- **Factibilidad:** Las soluciones de respaldo en la nube y en sitios físicos son accesibles, permitiendo que UCOP establezca procedimientos escalables según el volumen de datos y presupuesto.

8. Monitoreo Continuo y Sistemas de Información de Seguridad (SIEM)

- **Descripción:** Las soluciones SIEM recopilan y analizan los registros de seguridad en tiempo real para detectar patrones de amenazas.
- **Aplicación en UCOP:**
    - Implementación de un sistema SIEM para el monitoreo continuo de redes y aplicaciones críticas.
- **Factibilidad:** Las soluciones SIEM pueden ser escalables y gestionadas con proveedores externos, ajustándose a las limitaciones presupuestarias de UCOP y permitiendo la supervisión continua de los sistemas.

9. Capacitación y Concienciación en Seguridad para el Personal

- **Descripción:** La capacitación en ciberseguridad asegura que los empleados comprendan las políticas de seguridad y sus responsabilidades.
- **Aplicación en UCOP:**
    - Capacitación regular para todos los empleados en temas como phishing, gestión de contraseñas y mejores prácticas de seguridad.
- **Factibilidad:** La formación en seguridad puede realizarse mediante programas en línea, que son rentables y adaptables al personal de UCOP, promoviendo una cultura de seguridad con un bajo costo.

Factibilidad y Limitaciones Consideradas

Estos controles fueron seleccionados considerando los recursos de UCOP y las restricciones presupuestarias y operativas del sector público. Las soluciones propuestas incluyen opciones escalables, como servicios en la nube, que permiten una implementación gradual sin necesidad de grandes inversiones iniciales. Además, los controles como el cifrado, MFA y la capacitación en seguridad son efectivos para proteger los activos críticos y son viables dentro del marco de una organización pública con una estructura de TI limitada.

Resumen de Controles Seleccionados

Control de Seguridad	Aplicación en UCOP	Factibilidad
Firewall de Próxima Generación (NGFW)	Perímetro y áreas críticas	Gestión interna; escalabilidad en la red
Autenticación Multifactor (MFA)	Sistemas críticos	Compatible con sistemas actuales
Cifrado de Datos (en reposo y en tránsito)	Bases de datos, información de alto riesgo	Soluciones accesibles y escalables
Control de Acceso Basado en Roles (RBAC)	Datos y sistemas críticos	Soporte interno, adaptable a la estructura
Sistemas de Detección y Prevención de Intrusos (IDPS)	Red interna y perimetral	Escalable, gestionado en nube o local
Gestión de Parches y Actualizaciones	Todos los sistemas críticos	Programación interna; accesible
Respaldo y Recuperación de Datos	Sistemas críticos	Soluciones en la nube o físicas
Monitoreo Continuo y SIEM	Redes y aplicaciones críticas	Escalable, compatible con el presupuesto
Capacitación en Seguridad para el Personal	Todo el personal de UCOP	Económico, adaptable a necesidades públicas

---

Los controles de seguridad seleccionados cubren los riesgos críticos de UCOP y son compatibles con los recursos y limitaciones de una organización pública. Estos controles fortalecen la protección de datos críticos, garantizan el cumplimiento normativo y promueven una cultura de seguridad, asegurando la mitigación de los riesgos más apremiantes de UCOP.

Documentación de la Implementación de Controles de Seguridad para UCOP

Para UCOP, se detalla a continuación cada control de seguridad seleccionado, explicando cómo mitiga los riesgos correspondientes, junto con los roles y responsabilidades necesarios para su implementación.

1. Firewall de Próxima Generación (NGFW)

- **Descripción del Control:**
    - Los NGFW inspeccionan y filtran el tráfico de red, bloqueando amenazas avanzadas y accesos no autorizados en la red perimetral de UCOP.
    - **Mitigación del Riesgo:** Este control ayuda a proteger la red de accesos externos no autorizados y ataques externos, como ciberataques de malware y acceso no autorizado.
- **Roles y Responsabilidades:**
    - **Equipo de TI de Seguridad de Redes:** Configuración, gestión y monitoreo del firewall; realiza ajustes en la política de firewall según amenazas detectadas.
    - **Administrador de Sistemas:** Apoya en la configuración de reglas y monitoreo de logs del firewall.

2. Autenticación Multifactor (MFA)

- **Descripción del Control:**
    - MFA requiere que los usuarios verifiquen su identidad mediante varios métodos de autenticación, como una contraseña y un código enviado al teléfono.
    - **Mitigación del Riesgo:** Protege contra accesos no autorizados incluso si las contraseñas se ven comprometidas.

- **Roles y Responsabilidades:**
    - **Administrador de Seguridad de Identidad y Acceso (IAM):** Configuración inicial del MFA en todos los sistemas críticos y soporte para problemas de acceso.
    - **Equipo de TI de Soporte al Usuario:** Asistencia en la capacitación de usuarios y solución de problemas técnicos de autenticación.

3. Cifrado de Datos Sensibles (en reposo y en tránsito)

- **Descripción del Control:**
    - Implementación de cifrado en los datos almacenados y en tránsito, asegurando que solo usuarios autorizados puedan acceder y leer los datos.
    - **Mitigación del Riesgo:** Protege datos personales y sensibles de accesos no autorizados y exposiciones de datos en caso de intercepciones.
- **Roles y Responsabilidades:**
    - **Administrador de Bases de Datos:** Configuración y gestión de cifrado en bases de datos críticas de UCOP.
    - **Equipo de TI de Redes:** Implementación de cifrado en la comunicación de red.
    - **Responsable de Cumplimiento de Seguridad:** Verifica que el cifrado cumpla con regulaciones y políticas internas.

4. Control de Acceso Basado en Roles (RBAC)

- **Descripción del Control:**
    - RBAC permite asignar permisos de acceso a los sistemas y datos en función de las funciones y roles de cada usuario.
    - **Mitigación del Riesgo:** Minimiza los riesgos de acceso no autorizado, limitando la exposición de datos solo al personal autorizado.
- **Roles y Responsabilidades:**
    - **Administrador de Seguridad de Acceso (IAM):** Define y gestiona los roles de acceso en función de la estructura organizacional.

- **Supervisores de Departamento:** Supervisan el acceso adecuado de sus equipos y comunican al equipo de IAM cualquier cambio de roles.

5. Sistemas de Detección y Prevención de Intrusos (IDPS)

- **Descripción del Control:**
  - IDPS monitorea la red en tiempo real para detectar y bloquear ataques potenciales, analizando patrones de tráfico y comportamiento.
  - **Mitigación del Riesgo:** Ayuda a prevenir accesos no autorizados y ciberataques mediante la detección temprana y la respuesta a actividades sospechosas.
- **Roles y Responsabilidades:**
  - **Analista de Seguridad de Redes:** Configura, monitorea y responde a alertas generadas por el IDPS.
  - **Administrador de Redes:** Proporciona soporte para configurar el IDPS en puntos críticos de la red.

6. Gestión de Parches y Actualizaciones

- **Descripción del Control:**
  - La gestión de parches asegura que todos los sistemas críticos estén actualizados con los parches de seguridad más recientes para evitar la explotación de vulnerabilidades conocidas.
  - **Mitigación del Riesgo:** Reduce la exposición a vulnerabilidades conocidas y previene ataques que aprovechan sistemas desactualizados.
- **Roles y Responsabilidades:**
  - **Administrador de Sistemas:** Identifica e implementa actualizaciones en servidores y aplicaciones críticas.
  - **Equipo de Seguridad de TI:** Monitorea las alertas de vulnerabilidades y supervisa la aplicación de parches.
  - **Supervisor de TI:** Coordina y aprueba el calendario de parches según la disponibilidad de recursos.

7. Respaldo y Recuperación de Datos

- **Descripción del Control:**
    - La implementación de copias de seguridad diarias y planes de recuperación asegura que los datos se recuperen en caso de ataque o desastre.
    - **Mitigación del Riesgo:** Protege la disponibilidad de datos y asegura la continuidad del negocio en caso de pérdida de datos o interrupción del servicio.
- **Roles y Responsabilidades:**
    - **Administrador de Respaldo de Datos:** Configura y gestiona el proceso de respaldo de los sistemas críticos.
    - **Responsable de Recuperación de Desastres (DR):** Verifica la integridad de los respaldos y supervisa las pruebas de recuperación.
    - **Equipo de TI de Soporte:** Realiza pruebas de recuperación de datos según el plan de recuperación ante desastres.

8. Monitoreo Continuo y Sistema de Información de Seguridad (SIEM)

- **Descripción del Control:**
    - Un sistema SIEM recopila, analiza y correlaciona registros de eventos de seguridad en tiempo real para detectar patrones sospechosos.
    - **Mitigación del Riesgo:** Permite la detección proactiva y la rápida respuesta a incidentes de seguridad.
- **Roles y Responsabilidades:**
    - **Analista de Seguridad SIEM:** Monitorea y analiza las alertas y eventos generados por el SIEM, respondiendo a incidentes en tiempo real.
    - **Responsable del SOC (Centro de Operaciones de Seguridad):** Supervisa el equipo de SIEM y coordina las acciones de respuesta a incidentes.

9. Capacitación y Concienciación en Seguridad para el Personal

- **Descripción del Control:**
    - Programa de capacitación en ciberseguridad para educar a los empleados en mejores prácticas de seguridad, como detección de phishing y manejo de contraseñas.
    - **Mitigación del Riesgo:** Reduce riesgos de ingeniería social y errores humanos mediante la concienciación y capacitación del personal.
- **Roles y Responsabilidades:**
    - **Coordinador de Capacitación en Seguridad:** Diseña e implementa el programa de capacitación para todo el personal.
    - **Supervisores de Departamento:** Aseguran que sus equipos completen la capacitación en los tiempos definidos.
    - **Equipo de Cumplimiento de Seguridad:** Verifica que el programa cumpla con las políticas y normas de seguridad de UCOP.

Resumen de Roles y Responsabilidades

Control	Rol Principal	Responsabilidades de Soporte
Firewall NGFW	Equipo de TI de Seguridad de Redes	Administrador de Sistemas
Autenticación Multifactor (MFA)	Administrador IAM	Equipo de TI de Soporte al Usuario
Cifrado de Datos	Administrador de Bases de Datos	Equipo de TI de Redes, Responsable de Cumplimiento
Control de Acceso Basado en Roles	Administrador IAM	Supervisores de Departamento
Sistemas de Detección y Prevención	Analista de Seguridad de Redes	Administrador de Redes
Gestión de Parches	Administrador de Sistemas	Equipo de Seguridad de TI, Supervisor de TI
Respaldo y Recuperación de Datos	Administrador de Respaldo de Datos	Responsable de DR, Equipo de TI de Soporte
Monitoreo Continuo y SIEM	Analista de Seguridad SIEM	Responsable del SOC
Capacitación en Seguridad	Coordinador de Capacitación en Seguridad	Supervisores de Departamento, Equipo de Cumplimiento

Esta documentación de la implementación de controles define los pasos y roles necesarios para mitigar los riesgos en UCOP. La asignación de responsabilidades asegura que cada control esté adecuadamente gestionado y mantenido, alineando los recursos de la organización para maximizar la seguridad de la información.

Plan de Implementación de Controles de Seguridad para UCOP

Este plan establece un cronograma detallado para implementar los controles seleccionados, con recursos necesarios, dependencias y requisitos previos. La implementación sigue una estructura por fases, asegurando que cada control sea gestionado adecuadamente dentro de los recursos y limitaciones de UCOP.

Fase 1: Preparación (Mes 1 - Mes 2)

1. Revisión de Normas y Selección de Herramientas

- **Actividad:** Seleccionar herramientas específicas de acuerdo con las normas ISO 27001, NIST y CIS para implementar los controles necesarios.
- **Recursos:** Equipo de TI, responsables de cumplimiento, consultores de seguridad.
- **Duración:** 3 semanas.

2. Evaluación de Dependencias

- **Actividad:** Identificar sistemas críticos, dependencias técnicas y evaluar si se requieren actualizaciones o integraciones adicionales.
- **Recursos:** Equipo de TI, administradores de sistemas.
- **Duración:** 1 semana.

Fase 2: Implementación Inicial (Mes 3 - Mes 5)

1. Implementación de Firewalls de Próxima Generación (NGFW)

- **Cronograma:** Mes 3
- **Recursos Necesarios:** Equipo de TI de seguridad de redes, administradores de sistemas, NGFW de proveedores aprobados.
- **Dependencias:** Necesidad de definir reglas y políticas de seguridad en la red, infraestructura de red estable.
- **Requisito Previo:** Evaluación de la arquitectura de red para asegurar compatibilidad con los NGFW.

2. Implementación de Autenticación Multifactor (MFA)

- **Cronograma:** Mes 3 a Mes 4
- **Recursos Necesarios:** Equipo de TI de identidad y acceso, administradores de sistemas, licencias de solución MFA.
- **Dependencias:** Integración de MFA con sistemas críticos (financieros, recursos humanos).

- **Requisito Previo:** Revisión de compatibilidad de sistemas críticos con MFA.

3. Configuración de Cifrado de Datos Sensibles (en reposo y en tránsito)

- **Cronograma:** Mes 4 a Mes 5
- **Recursos Necesarios:** Administradores de bases de datos, equipo de TI de redes, herramientas de cifrado y administración de claves.
- **Dependencias:** Configuración de cifrado en bases de datos, servidores y almacenamiento en la nube.
- **Requisito Previo:** Identificación de datos sensibles y selección de algoritmos de cifrado compatibles.

Fase 3: Implementación Avanzada (Mes 6 - Mes 9)

1. Configuración de Control de Acceso Basado en Roles (RBAC)

- **Cronograma:** Mes 6
- **Recursos Necesarios:** Administradores de IAM, supervisores de departamento, software de gestión de accesos.
- **Dependencias:** Integración de RBAC con sistemas existentes de gestión de usuarios.
- **Requisito Previo:** Identificación y definición de roles y permisos para cada departamento y usuario.

2. Implementación de Sistemas de Detección y Prevención de Intrusos (IDPS)

- **Cronograma:** Mes 6 a Mes 7
- **Recursos Necesarios:** Analistas de seguridad de redes, administradores de redes, licencias de software IDPS.
- **Dependencias:** Configuración de sensores en los puntos críticos de la red interna y perimetral.
- **Requisito Previo:** Definir políticas de detección y respuesta basadas en los patrones de tráfico de la organización.

3. Establecimiento de Gestión de Parches y Actualizaciones

- **Cronograma:** Mes 7 a Mes 8
- **Recursos Necesarios:** Administradores de sistemas, equipo de seguridad de TI, herramientas de gestión de parches.

- **Dependencias:** Identificación de software crítico y servidores que requieren actualizaciones regulares.
- **Requisito Previo:** Creación de un inventario actualizado de sistemas y aplicaciones que necesiten parches.

4. Implementación de Respaldo y Recuperación de Datos

- **Cronograma:** Mes 8 a Mes 9
- **Recursos Necesarios:** Administrador de respaldo de datos, responsable de recuperación de desastres (DR), soluciones de respaldo en la nube y físicas.
- **Dependencias:** Establecimiento de un calendario de respaldo y configuración de almacenamiento seguro.
- **Requisito Previo:** Identificación de sistemas críticos y prueba inicial de recuperación de datos para evaluar la eficacia de la estrategia.

Fase 4: Monitoreo y Capacitación (Mes 10 - Mes 12)

1. Configuración de Monitoreo Continuo y SIEM

- **Cronograma:** Mes 10 a Mes 11
- **Recursos Necesarios:** Analista de seguridad SIEM, equipo de SOC, licencias de SIEM.
- **Dependencias:** Integración con sistemas críticos para análisis en tiempo real y generación de alertas.
- **Requisito Previo:** Configuración inicial de parámetros de alerta y pruebas de detección para verificar el correcto funcionamiento del SIEM.

2. Capacitación en Seguridad y Concienciación para el Personal

- **Cronograma:** Mes 11 a Mes 12
- **Recursos Necesarios:** Coordinador de capacitación en seguridad, plataforma de aprendizaje en línea, supervisores de departamento.
- **Dependencias:** Coordinación de horarios para asegurar la disponibilidad de los empleados.
- **Requisito Previo:** Desarrollo de materiales de capacitación en seguridad y aprobación de los temas de capacitación por el equipo de cumplimiento.

Resumen del Plan de Implementación

Control de Seguridad	Cronograma	Recursos Necesarios	Dependencias	Requisito Previo
Firewalls NGFW	Mes 3	Equipo de seguridad de redes, NGFW	Políticas de seguridad definidas	Evaluación de arquitectura de red
Autenticación Multifactor (MFA)	Mes 3 - Mes 4	Equipo de IAM, licencias MFA	Integración con sistemas críticos	Compatibilidad con sistemas críticos
Cifrado de Datos Sensibles	Mes 4 - Mes 5	Administradores de BD, herramientas de cifrado	Configuración en bases de datos y servidores	Identificación de datos y selección de algoritmos
Control de Acceso Basado en Roles (RBAC)	Mes 6	Administradores IAM, software de gestión de accesos	Integración con gestión de usuarios	Definición de roles y permisos
Sistemas de Detección y Prevención (IDPS)	Mes 6 - Mes 7	Analistas de seguridad, licencias IDPS	Configuración en red interna y perimetral	Definir políticas de detección
Gestión de Parches y Actualizaciones	Mes 7 - Mes 8	Administradores de sistemas, herramientas de parches	Identificación de software y servidores críticos	Inventario de sistemas y aplicaciones
Respaldo y Recuperación de Datos	Mes 8 - Mes 9	Administrador de respaldo, soluciones en nube/físicas	Calendario de respaldo y configuración de almacenamiento	Identificación de sistemas críticos
Monitoreo Continuo y SIEM	Mes 10 - Mes 11	Analista SIEM, equipo SOC	Integración con sistemas críticos	Configuración inicial de alertas

Control de Seguridad	Cronograma	Recursos Necesarios	Dependencias	Requisito Previo
				y pruebas de detección
Capacitación en Seguridad	Mes 11 - Mes 12	Coordinador de capacitación, plataforma de e-learning	Coordinación de horarios de capacitación	Desarrollo y aprobación de materiales

---

Este plan de implementación detalla los pasos necesarios para implementar cada control de seguridad en UCOP, con una estrategia que asegura el cumplimiento normativo, la continuidad operativa y la protección de los datos críticos. Los cronogramas y recursos asignados están diseñados para cumplir con los requisitos del sector público y optimizar los recursos existentes en UCOP.

4.- Documentación de Políticas y Procedimientos de Seguridad para UCOP

Basado en la página de UCOP (https://security.ucop.edu/index.html), se presenta a continuación un marco formal para documentar las políticas y procedimientos de seguridad. Esta documentación asegura que UCOP mantenga prácticas consistentes, efectivas y alineadas con las normativas de seguridad para proteger sus activos críticos.

1. Política de Seguridad de la Información

Propósito:

Definir el compromiso de UCOP con la seguridad de la información, estableciendo directrices claras para proteger la confidencialidad, integridad y disponibilidad de los datos críticos de la institución.

Principios Clave:

- **Confidencialidad:** Garantizar que el acceso a la información esté limitado solo a personas autorizadas.
- **Integridad:** Proteger la precisión y la totalidad de la información y los métodos de procesamiento.
- **Disponibilidad:** Asegurar que la información y los sistemas estén accesibles para los usuarios autorizados cuando se necesiten.

Alcance:

Aplica a todos los empleados, contratistas y terceros que interactúan con los activos de información de UCOP.

Procedimientos:

- Todos los usuarios deben seguir los procedimientos de control de acceso establecidos y usar autenticación multifactor (MFA) para acceder a sistemas críticos.
- La información sensible debe estar cifrada en reposo y en tránsito.

- Los datos deben ser gestionados de acuerdo con las políticas de retención y eliminación de UCOP.

2. Política de Control de Acceso

Propósito:

Establecer procedimientos para gestionar y controlar el acceso de usuarios a los sistemas y datos críticos de UCOP, minimizando los riesgos de acceso no autorizado.

Directrices:

- **Control de Acceso Basado en Roles (RBAC):** El acceso a los sistemas debe basarse en las funciones de los empleados, limitando el acceso a la información necesaria para cumplir con sus responsabilidades laborales.
- **Gestión de Contraseñas y Autenticación Multifactor (MFA):** Todos los usuarios deben utilizar contraseñas complejas y autenticación multifactor en los sistemas críticos.

Procedimientos:

- **Creación de cuentas:** Las cuentas de usuario deben crearse con los permisos mínimos necesarios y ser revisadas regularmente.
- **Auditoría de Accesos:** Realizar auditorías periódicas de los accesos a sistemas críticos y revocar los permisos de usuarios que ya no necesitan acceso.

3. Política de Cifrado de Datos

Propósito:

Asegurar que todos los datos sensibles de UCOP estén protegidos mediante cifrado para prevenir accesos no autorizados.

Directrices:

- **Cifrado en Reposo y en Tránsito:** Todos los datos sensibles, incluyendo información personal, financiera y de investigación, deben cifrarse en reposo y durante la transmisión.
- **Gestión de Claves de Cifrado:** Las claves de cifrado deben gestionarse y almacenarse de forma segura, con acceso limitado al personal autorizado.

Procedimientos:

- **Implementación de Cifrado:** Los administradores de bases de datos y redes deben aplicar cifrado en todos los sistemas y bases de datos que contienen información sensible.
- **Pruebas de Cifrado:** Verificar regularmente la efectividad de las configuraciones de cifrado y ajustar las políticas cuando sea necesario.

4. Política de Respaldo y Recuperación de Datos

Propósito:

Establecer un marco para el respaldo regular y la recuperación de los datos críticos de UCOP para asegurar la continuidad del negocio.

Directrices:

- **Frecuencia de Respaldo:** Los sistemas críticos deben tener copias de seguridad diarias, y los datos menos sensibles deben respaldarse semanalmente.
- **Pruebas de Recuperación de Datos:** Se deben realizar pruebas de recuperación de datos trimestralmente para asegurar la eficacia del plan de recuperación.

Procedimientos:

- **Implementación de Respaldo:** Los administradores de sistemas deben programar respaldos automáticos y verificar que se almacenen en ubicaciones seguras.
- **Restauración de Datos:** El equipo de TI debe seguir un procedimiento documentado para restaurar los datos en caso de una interrupción.

5. Política de Gestión de Incidentes de Seguridad

Propósito:

Definir un proceso para identificar, responder y mitigar los incidentes de seguridad que puedan afectar a los sistemas y datos de UCOP.

Directrices:

- **Detección de Incidentes:** Implementar monitoreo continuo mediante sistemas SIEM e IDPS para detectar incidentes de seguridad.
- **Gestión de Incidentes:** Seguir un proceso estructurado para contener, erradicar y recuperar los sistemas afectados por un incidente.

Procedimientos:

- **Notificación de Incidentes:** Los empleados deben informar inmediatamente sobre cualquier incidente de seguridad al equipo de seguridad de la información.
- **Análisis de Incidentes:** El equipo de respuesta a incidentes (IRT) debe analizar y documentar todos los incidentes para identificar las causas y evitar su recurrencia.
- **Reporte de Incidentes:** Todos los incidentes deben documentarse, y los incidentes de alto riesgo deben reportarse a la dirección ejecutiva.

6. Política de Capacitación en Seguridad de la Información

Propósito:

Fomentar una cultura de seguridad mediante la capacitación continua del personal en prácticas de seguridad de la información.

Directrices:

- **Frecuencia de Capacitación:** Todos los empleados deben recibir capacitación anual en temas de seguridad de la información, incluyendo la detección de phishing, gestión de contraseñas y prácticas de seguridad.
- **Capacitación Especializada:** El personal de TI y de alto riesgo debe recibir capacitación adicional en temas avanzados de seguridad.

Procedimientos:

- **Implementación de Capacitación:** El coordinador de capacitación en seguridad de TI debe organizar sesiones de capacitación presenciales y en línea.
- **Evaluación de Conocimientos:** Realizar evaluaciones de conocimiento al finalizar cada capacitación para asegurar que los empleados comprendan y apliquen las prácticas de seguridad.

7. Política de Gestión de Parches y Actualizaciones

Propósito:

Asegurar que todos los sistemas y aplicaciones de UCOP estén actualizados con los parches de seguridad más recientes para prevenir la explotación de vulnerabilidades.

Directrices:

- **Actualización Regular:** Todos los sistemas críticos deben recibir actualizaciones de seguridad mensuales y los sistemas no críticos, trimestrales.
- **Gestión de Vulnerabilidades:** Se debe realizar un análisis regular de vulnerabilidades y aplicar parches según la prioridad de cada sistema.

Procedimientos:

- **Revisión de Parches Disponibles:** El equipo de TI revisa las actualizaciones disponibles y evalúa la necesidad de aplicar cada parche.
- **Implementación de Parches:** Los parches de seguridad deben aplicarse en un entorno de pruebas antes de implementarse en producción para evitar interrupciones.

8. Política de Privacidad de Datos

Propósito:

Establecer directrices para proteger la privacidad de los datos personales de los estudiantes, empleados y ciudadanos que UCOP maneja.

Directrices:

- **Acceso Restringido:** Limitar el acceso a los datos personales solo al personal autorizado y en función de sus responsabilidades laborales.
- **Retención y Eliminación de Datos:** Establecer períodos de retención claros y eliminar los datos personales que ya no sean necesarios.

Procedimientos:

- **Gestión de Datos Personales:** Los sistemas deben configurarse para cumplir con las políticas de retención y eliminación de datos de UCOP.
- **Auditorías de Privacidad:** Realizar auditorías periódicas para verificar el cumplimiento con las políticas de privacidad y ajustar las prácticas si es necesario.

Estas políticas y procedimientos proporcionan un marco de control que guía a UCOP en la protección de su información crítica, alineándose con los estándares y normativas de seguridad. La documentación formal garantiza la consistencia en la aplicación de medidas de seguridad y el cumplimiento de los requisitos de confidencialidad, integridad y disponibilidad de los datos. Esta estructura no solo protege los sistemas de UCOP, sino que también fomenta una cultura de seguridad entre todos los miembros de la organización.

Política de Seguridad de la Información de UCOP

Propósito: La University of California Office of the President (UCOP) se compromete a proteger la seguridad de la información que maneja, asegurando que los datos críticos y confidenciales se gestionen de acuerdo con los más altos estándares de seguridad. Esta política de seguridad establece los principios fundamentales y el compromiso de UCOP para garantizar la **confidencialidad**, **integridad** y **disponibilidad** de sus activos de información, en alineación con las normativas aplicables y las mejores prácticas de la industria.

Alcance:

Esta política se aplica a todos los empleados, contratistas, consultores y terceros que tienen acceso a los sistemas de información, datos y activos críticos de UCOP. La política cubre todos los aspectos de seguridad en los sistemas, redes y dispositivos que UCOP utiliza para su operación y gestión.

Principios Clave

1. **Confidencialidad**
    - UCOP garantiza que la información crítica, confidencial y personal de estudiantes, empleados y terceros esté protegida de accesos no autorizados.
    - Se implementarán controles de acceso, autenticación multifactor (MFA) y cifrado de datos para asegurar que solo las personas autorizadas puedan acceder a la información necesaria para su rol.
2. **Integridad**
    - UCOP mantiene la precisión y totalidad de la información en sus sistemas, asegurando que los datos no sean alterados sin autorización o conocimiento.

    - Se aplicarán procedimientos de auditoría y control de acceso para proteger la integridad de la información, junto con procesos de respaldo y recuperación para preservar la consistencia de los datos.

3. **Disponibilidad**
    - UCOP se compromete a asegurar que la información y los sistemas estén disponibles para los usuarios autorizados cuando se necesiten para el cumplimiento de sus funciones.
    - Mediante planes de respaldo, continuidad de negocio y recuperación ante desastres, UCOP garantiza que la información esté accesible y los sistemas sean resilientes ante fallos y amenazas.

Compromiso de Cumplimiento

UCOP se compromete a cumplir con todas las leyes, regulaciones y estándares aplicables, tales como **FERPA** para la protección de datos estudiantiles y **HIPAA** para la información de salud. Todos los empleados y terceros deben adherirse a esta política y a los procedimientos de seguridad establecidos por la organización.

Roles y Responsabilidades

- **Dirección Ejecutiva:** Asegurar los recursos necesarios para implementar esta política y supervisar su cumplimiento.
- **Equipo de TI y Seguridad de la Información:** Implementar, monitorear y mejorar los controles de seguridad, alineados con los principios de confidencialidad, integridad y disponibilidad.
- **Todos los Empleados y Contratistas:** Seguir las prácticas de seguridad de UCOP, reportar incidentes y cumplir con los procedimientos establecidos para proteger la información.

Revisión y Mejora Continua

La política de seguridad de UCOP será revisada y actualizada anualmente, o en caso de cambios significativos en la normativa o tecnología, para asegurar que se mantenga alineada con las mejores prácticas y los objetivos de la organización. UCOP está comprometido con la mejora continua de su sistema de seguridad de la información.

Esta Política de Seguridad de la Información reafirma el compromiso de UCOP con la protección de su información y recursos críticos, promoviendo una cultura de seguridad que garantice la confianza y el cumplimiento de las expectativas de sus estudiantes, empleados y comunidad.

Política de Control de Acceso de Usuarios de UCOP

Propósito:
Esta política establece los lineamientos para conceder, modificar y revocar el acceso de los usuarios a los sistemas y datos de UCOP, así como los requisitos para la creación y gestión de contraseñas, asegurando que se mantenga la confidencialidad, integridad y disponibilidad de la información crítica.

1. Concesión, Modificación y Revocación del Acceso de Usuarios

Concesión de Acceso

- **Proceso de Solicitud de Acceso:** Los supervisores deben solicitar el acceso de los nuevos usuarios mediante un formulario oficial, especificando el nivel de acceso requerido en función de las responsabilidades laborales del empleado.
- **Principio de Privilegio Mínimo:** El acceso se otorgará únicamente al mínimo necesario para cumplir con las funciones laborales, siguiendo un modelo de Control de Acceso Basado en Roles (RBAC).
- **Autenticación Multifactor (MFA):** Todos los accesos a sistemas críticos deben ser protegidos mediante MFA.

Modificación del Acceso

- **Reevaluación del Acceso:** Los supervisores deben comunicar cualquier cambio en las funciones o responsabilidades laborales del usuario al equipo de seguridad, que ajustará los permisos en función de las nuevas responsabilidades.
- **Proceso de Actualización de Roles:** Los cambios en el acceso serán registrados en el sistema de gestión de identidad y acceso (IAM) y aprobados por el supervisor correspondiente.

Revocación del Acceso

- **Revocación Inmediata:** Cuando un usuario deja de estar afiliado a UCOP (terminación de contrato, cambio de rol), el acceso debe ser revocado inmediatamente por el equipo de seguridad.
- **Proceso de Cierre de Cuenta:** Se revisará cada cuenta eliminada para verificar la revocación de todos los permisos y accesos en todos los sistemas.
- **Auditoría de Cuentas Inactivas:** Cualquier cuenta que no haya sido utilizada en un periodo de 90 días será desactivada automáticamente y revisada.

2. Política de Contraseñas

Requisitos de Complejidad

Para proteger la información y los sistemas críticos, las contraseñas deben cumplir con los siguientes requisitos de complejidad:

- **Longitud Mínima:** Las contraseñas deben tener al menos 12 caracteres.
- **Variedad de Caracteres:** Deben incluir al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (por ejemplo, !, @, #).
- **Prohibición de Contraseñas Comunes:** No se permiten contraseñas de uso común ni secuencias como "1234", "password", o palabras derivadas del nombre de usuario o de la organización.
- **Reutilización de Contraseñas:** No se permite el uso de las últimas cinco contraseñas.

Frecuencia de Rotación

- **Cambio de Contraseña Obligatorio:** Todos los usuarios deben cambiar su contraseña cada 90 días.
- **Cambio de Contraseña en Caso de Incidente:** Si se detecta un incidente de seguridad relacionado con las credenciales de usuario, se debe restablecer la contraseña de inmediato.
- **Notificaciones de Vencimiento:** Los usuarios recibirán notificaciones automáticas de vencimiento de contraseña 14 días antes de la fecha límite para cambiarla.

Roles y Responsabilidades

- **Supervisores:** Solicitar accesos iniciales y comunicar cualquier cambio en los roles de los empleados.

- **Equipo de Seguridad de TI:** Otorgar, modificar y revocar accesos en función de las solicitudes aprobadas y mantener la administración de contraseñas.
- **Todos los Usuarios:** Cumplir con las políticas de contraseñas y responder puntualmente a las solicitudes de cambio de contraseña o ajustes de acceso.

Revisión y Monitoreo

El equipo de seguridad realizará auditorías trimestrales para revisar el acceso de los usuarios y verificar el cumplimiento de la política de contraseñas. Las excepciones a esta política deben ser justificadas y aprobadas por la dirección de TI de UCOP.

Esta Política de Control de Acceso de Usuarios asegura que los accesos se gestionen de manera segura y que las contraseñas cumplan con los requisitos necesarios para proteger la información de UCOP.

Plan de Respuesta a Incidentes de UCOP

Este plan establece los lineamientos y procedimientos para identificar, responder, mitigar y documentar los incidentes de seguridad en UCOP. El objetivo es reducir el impacto de los incidentes de seguridad y restaurar rápidamente las operaciones normales, garantizando la protección de los activos de información.

1. Definición de Incidente de Seguridad

Un **incidente de seguridad** es cualquier evento inesperado que compromete o podría comprometer la **confidencialidad**, **integridad** o **disponibilidad** de la información, sistemas, redes o infraestructura de UCOP. Ejemplos incluyen:

- Acceso no autorizado a sistemas o datos.
- Malware o ransomware que afecta la funcionalidad de sistemas.
- Pérdida o robo de dispositivos que contienen datos críticos.
- Exposición de datos personales o confidenciales.
- Violaciones de políticas de seguridad, como el uso indebido de contraseñas.

- Ciberataques, como ataques de denegación de servicio (DoS) o intentos de phishing.

2. Procedimiento de Respuesta a Incidentes

Paso 1: Identificación y Notificación

- **Detección:** Los empleados deben estar alertas a posibles indicios de incidentes, como actividad inusual en el sistema, alertas de seguridad y errores de sistema.
- **Notificación Inmediata:** Al identificar un posible incidente, el empleado debe notificar inmediatamente al Equipo de Respuesta a Incidentes (IRT) a través del canal de comunicación designado (correo de incidentes o línea de emergencia).
- **Registro del Incidente:** El IRT registra el incidente en el sistema de gestión de incidentes, anotando detalles iniciales como fecha, hora, sistema afectado y descripción del evento.

Paso 2: Contención

- **Contención Inicial:** Aislar el sistema afectado (por ejemplo, desconectarlo de la red) para evitar la propagación del incidente a otros sistemas o datos.
- **Contención a Corto Plazo:** Si el incidente es grave, implementar medidas temporales (como desactivar cuentas comprometidas) para mitigar el impacto mientras se investiga la causa.
- **Evaluación de Riesgos:** El IRT evalúa el alcance del incidente para determinar el nivel de impacto y los recursos necesarios para gestionar la contención.

Paso 3: Análisis y Erradicación

- **Análisis Forense:** Realizar un análisis detallado para identificar el origen, la causa y el impacto del incidente. Esto puede incluir la revisión de registros, análisis de sistemas y entrevistas con usuarios involucrados.
- **Erradicación del Incidente:** Eliminar cualquier elemento dañino, como malware, y aplicar parches o actualizaciones para corregir las vulnerabilidades que causaron el incidente.

- **Restablecimiento de Sistemas:** Asegurar que todos los sistemas se restauren a su estado seguro antes de reanudar las operaciones.

Paso 4: Recuperación

- **Reinstalación de Sistemas:** Restaurar sistemas afectados mediante copias de seguridad verificadas para garantizar que estén libres de cualquier código malicioso.
- **Pruebas de Seguridad:** Realizar pruebas de seguridad para validar que los sistemas están completamente operativos y seguros antes de ponerlos en producción.
- **Monitoreo Post-Incidente:** Mantener un monitoreo intensivo de los sistemas afectados para detectar cualquier actividad inusual que indique una posible reaparición del incidente.

Paso 5: Documentación y Aprendizaje

- **Informe del Incidente:** El IRT elabora un informe detallado del incidente que incluye las causas, el proceso de mitigación, el impacto y las acciones correctivas.
- **Revisión y Mejora:** Revisar las lecciones aprendidas y actualizar las políticas, procedimientos y controles de seguridad según los hallazgos del incidente.
- **Capacitación:** Si el incidente fue resultado de un error humano o de una falta de conocimiento, organizar capacitaciones para reforzar la seguridad entre el personal.

3. Roles y Responsabilidades en la Gestión de Incidentes

Equipo de Respuesta a Incidentes (IRT)

- **Responsabilidad Principal:** Detectar, contener y resolver los incidentes de seguridad, trabajando en conjunto con otros departamentos según sea necesario.
- **Tareas Específicas:**
    - Recibir y gestionar las notificaciones de incidentes.
    - Realizar análisis forense y coordinar la erradicación y recuperación.
    - Documentar y elaborar informes detallados de cada incidente.

Analista de Seguridad

- **Responsabilidad Principal:** Monitorear los sistemas y redes de UCOP en busca de actividades sospechosas.

- **Tareas Específicas:**
    - Configurar alertas en el sistema de gestión de eventos de seguridad (SIEM).
    - Apoyar en la identificación y análisis forense de los incidentes.

Administrador de Redes y Sistemas

- **Responsabilidad Principal:** Apoyar en la contención y recuperación de sistemas afectados.
- **Tareas Específicas:**
    - Aislar los sistemas comprometidos durante la contención inicial.
    - Colaborar en la reinstalación y prueba de los sistemas restaurados.

Liderazgo de UCOP

- **Responsabilidad Principal:** Asegurar la disponibilidad de recursos y supervisar la gestión de incidentes graves.
- **Tareas Específicas:**
    - Aprobar las decisiones estratégicas de mitigación de riesgos.
    - Revisar informes de incidentes de alto impacto y supervisar las mejoras necesarias.

Usuarios Finales

- **Responsabilidad Principal:** Reportar cualquier actividad sospechosa o incidente al IRT.
- **Tareas Específicas:**
    - Cooperar con el IRT durante el proceso de investigación del incidente.
    - Asistir en la capacitación en seguridad de la información.

Este Plan de Respuesta a Incidentes de UCOP proporciona un enfoque estructurado para gestionar incidentes de seguridad, asegurando que todos los miembros de la organización conozcan sus roles y responsabilidades en cada etapa. El seguimiento de este plan permite a UCOP responder de manera rápida y efectiva, minimizando el impacto de los incidentes y fortaleciendo su sistema de seguridad para prevenir futuros eventos.

Política de Copia de Seguridad y Recuperación de Datos de UCOP

Esta política establece los procedimientos para realizar copias de seguridad regulares de los datos críticos de UCOP y asegura que los datos puedan recuperarse de manera eficaz en caso de una interrupción o incidente de seguridad. La política también define los roles y responsabilidades en el proceso de copia de seguridad y recuperación.

1. Procedimientos para Copias de Seguridad de Datos

Frecuencia de Copias de Seguridad

- **Copias de Seguridad Diarias:** Se realizarán copias de seguridad diarias para sistemas críticos, incluyendo bases de datos de estudiantes, sistemas financieros y aplicaciones administrativas.
- **Copias de Seguridad Semanales:** Para datos de menor criticidad, como archivos de referencia y sistemas de soporte, las copias de seguridad se realizarán semanalmente.
- **Copias de Seguridad Mensuales:** Copias de seguridad de archivos de archivo o datos de bajo uso, que pueden ser necesarios para auditorías o referencias ocasionales, se realizarán mensualmente y se almacenarán a largo plazo.

Almacenamiento de Copias de Seguridad

- **Ubicación Principal de Respaldo:** Las copias de seguridad se almacenarán en un centro de datos seguro ubicado en una instalación de UCOP.
- **Ubicación Secundaria (Backup en la Nube):** Las copias de seguridad críticas serán replicadas en un servicio de almacenamiento en la nube seguro para asegurar su disponibilidad en caso de desastre.

- **Retención de Copias de Seguridad:** Las copias diarias se retendrán durante 30 días, las semanales por 6 meses y las mensuales durante 1 año, con revisiones periódicas para determinar si es necesario extender la retención.

Procedimiento de Copia de Seguridad

1. **Planificación y Programación:** Las copias de seguridad estarán programadas en el sistema de gestión de copias para ejecutarse automáticamente fuera del horario laboral, reduciendo el impacto en el rendimiento del sistema.
2. **Verificación de Copias de Seguridad:** Después de cada copia de seguridad, el sistema generará un reporte automático de verificación para asegurar la integridad y completitud de los datos.
3. **Notificación de Fallos:** En caso de que una copia de seguridad falle, el administrador de respaldo recibirá una notificación inmediata para realizar una copia manual y analizar la causa del fallo.

2. Procedimientos de Recuperación de Datos

Pruebas de Recuperación

- **Pruebas Trimestrales:** Las pruebas de recuperación se realizarán trimestralmente en datos críticos, verificando que los datos pueden restaurarse de manera completa y funcional.
- **Pruebas de Escenarios de Desastres:** Anualmente, UCOP realizará un simulacro de recuperación ante desastres para asegurar que los procedimientos de recuperación sean efectivos en situaciones de emergencia y que todos los sistemas críticos puedan restaurarse en un periodo razonable.

Proceso de Recuperación de Datos

1. **Solicitud de Recuperación:** En caso de pérdida de datos, el equipo responsable deberá enviar una solicitud formal al administrador de respaldo.
2. **Validación de Autenticidad:** Antes de la recuperación, se verificará la autenticidad de la solicitud para evitar restauraciones no autorizadas.
3. **Restauración de Datos:** Los administradores de sistemas restaurarán los datos desde la última copia de seguridad válida y completarán la restauración en coordinación con los usuarios afectados.
4. **Verificación Post-Recuperación:** Una vez completada la restauración, los administradores verificarán la integridad y consistencia de los datos restaurados.

Roles y Responsabilidades

Administrador de Respaldo de Datos

- **Responsabilidades:**
    - Configuración y mantenimiento de los sistemas de respaldo y restauración de datos.
    - Revisión diaria de los reportes de copias de seguridad y notificación de cualquier fallo.
    - Ejecución de pruebas de recuperación trimestrales y anuales.
- **Contacto:** Disponible para resolver cualquier incidencia de respaldo y para coordinar la restauración en caso de incidentes.

Equipo de Seguridad de TI

- **Responsabilidades:**
    - Monitorear el cumplimiento de la política de copia de seguridad y recuperación.
    - Coordinar el simulacro anual de recuperación ante desastres.
    - Supervisar el almacenamiento seguro de las copias en la nube y en instalaciones secundarias.

Usuarios de Datos Críticos

- **Responsabilidades:**
    - Notificar al equipo de TI en caso de pérdida de datos o incidente que afecte la integridad de los sistemas.
    - Colaborar con el equipo de TI durante el proceso de recuperación para validar que los datos restaurados cumplen con los requisitos.

Director de TI

- **Responsabilidades:**
    - Aprobar el calendario de pruebas de recuperación y el simulacro de desastres.
    - Revisar informes de recuperación y restauración de datos para verificar la efectividad del proceso y autorizar cualquier ajuste necesario en los procedimientos.

Conclusión

Esta Política de Copia de Seguridad y Recuperación de Datos de UCOP asegura la protección de la información crítica y garantiza la continuidad de las operaciones en caso de pérdida de datos o interrupciones. Con procedimientos definidos, pruebas de recuperación regulares y roles claramente establecidos, UCOP puede asegurar que sus datos estarán disponibles, íntegros y protegidos frente a posibles desastres o incidentes de seguridad.

Plan de Concienciación y Capacitación en Seguridad para Empleados de UCOP

El objetivo de este plan es asegurar que todos los empleados de UCOP comprendan las políticas de seguridad de la organización, sus responsabilidades para proteger los datos críticos y las mejores prácticas de seguridad que deben seguir en sus actividades diarias. Mediante capacitación continua y materiales de concienciación, UCOP busca crear una cultura de seguridad en toda la organización.

1. Plan de Capacitación en Seguridad de la Información

A. Objetivos de la Capacitación

- Asegurar que los empleados conozcan y comprendan las políticas de seguridad de UCOP, incluyendo control de acceso, manejo de contraseñas y procedimientos de respuesta a incidentes.
- Capacitar a los empleados en la identificación de amenazas comunes, como el phishing, y en cómo reportar posibles incidentes de seguridad.
- Promover el compromiso y la participación de todos los empleados en el mantenimiento de la seguridad de la información.

B. Estructura de la Capacitación

1. **Capacitación de Introducción a la Seguridad de la Información**
    - **Público Objetivo:** Nuevos empleados (durante la primera semana de ingreso).
    - **Contenido:**
        - Introducción a las políticas de seguridad de UCOP.

        - Explicación de las responsabilidades de los empleados en cuanto a la protección de la información.
        - Guía para el uso seguro de contraseñas, control de acceso y uso de MFA.
    - **Duración:** 1 hora.
    - **Formato:** Sesión virtual o presencial.
2. **Capacitación Anual en Seguridad de la Información**
    - **Público Objetivo:** Todos los empleados.
    - **Contenido:**
        - Actualización sobre las políticas de seguridad y procedimientos de UCOP.
        - Taller práctico de identificación de amenazas como phishing, malware y ransomware.
        - Procedimientos de respuesta a incidentes y cómo reportar actividad sospechosa.
    - **Duración:** 2 horas.
    - **Formato:** Sesión en línea interactiva.
3. **Capacitación Especializada para Equipos de Alto Riesgo**
    - **Público Objetivo:** Personal de TI, recursos humanos y finanzas, y cualquier otra área que maneje datos sensibles.
    - **Contenido:**
        - Análisis forense básico y protocolos de contención de incidentes.
        - Gestión segura de datos personales y confidenciales.
        - Uso de herramientas avanzadas de seguridad y monitoreo.
    - **Duración:** 4 horas.
    - **Formato:** Taller presencial o virtual con ejercicios prácticos.
4. **Recordatorios Mensuales de Seguridad**
    - **Público Objetivo:** Todos los empleados.

- **Contenido:** Breves recordatorios sobre temas clave de seguridad, como rotación de contraseñas, protección contra phishing y el uso adecuado del control de acceso.
- **Formato:** Boletines por correo electrónico.

2. Materiales de Concienciación para Fomentar las Mejores Prácticas de Seguridad

Para reforzar la capacitación y recordar a los empleados las prácticas de seguridad, se desarrollarán materiales de concienciación visuales y accesibles en toda la organización.

A. Carteles y Pósters de Seguridad

1. **"Protege Tu Contraseña"**
    - **Contenido:** Consejos para crear contraseñas seguras, evitar el uso de contraseñas comunes y cómo rotarlas cada 90 días.
    - **Ubicación:** Cerca de las áreas de trabajo y en las estaciones de inicio de sesión.
2. **"¿Reconoces un Correo Sospechoso?"**
    - **Contenido:** Ejemplos visuales de correos de phishing, recordando a los empleados no hacer clic en enlaces sospechosos y reportar cualquier correo inusual.
    - **Ubicación:** En los tablones de anuncios y áreas de descanso.
3. **"Mantén Tu Dispositivo Seguro"**
    - **Contenido:** Recordatorios sobre el uso de autenticación multifactor (MFA) y bloqueo de dispositivos al dejar el área de trabajo.
    - **Ubicación:** Cerca de las estaciones de trabajo y en salas de conferencias.

B. Guías y Directrices en Línea

1. **Guía de Buenas Prácticas en Seguridad Informática**

- **Contenido:** Directrices detalladas sobre el uso seguro de contraseñas, gestión de dispositivos, navegación segura y reporte de incidentes.
- **Formato:** Documento PDF disponible en la intranet y entregado a todos los empleados al inicio de su contratación.

2. **Manual de Respuesta a Incidentes para Empleados**
    - **Contenido:** Procedimientos básicos para que los empleados sepan cómo actuar y a quién notificar en caso de detectar actividad sospechosa o un incidente de seguridad.
    - **Formato:** Documento de referencia rápida en formato digital y físico en las áreas de trabajo.

3. **Infografías de Seguridad Mensuales**
    - **Contenido:** Mensajes visuales concisos sobre temas como el uso de MFA, cómo evitar ataques de ingeniería social y la importancia del cifrado.
    - **Formato:** Infografías compartidas por correo electrónico y disponibles en la intranet de UCOP.

C. Recordatorios Automáticos de Seguridad

- **Alertas de Cambio de Contraseña:** Recordatorios automatizados que se envían a los empleados 14 días antes de la expiración de su contraseña.
- **Alertas de Ciberseguridad Semanales:** Breves consejos de seguridad enviados por correo electrónico, cubriendo temas actuales de ciberseguridad y mejores prácticas.

Roles y Responsabilidades en la Capacitación de Seguridad

Coordinador de Capacitación en Seguridad

- **Responsabilidades:** Diseñar y actualizar el contenido de la capacitación; coordinar las sesiones de capacitación y distribuir los materiales de concienciación.
- **Contacto:** Responsable de resolver preguntas de los empleados sobre temas de capacitación en seguridad.

Supervisores de Departamento

- **Responsabilidades:** Asegurar que todos los empleados de su equipo completen la capacitación requerida y fomentar la participación en los programas de concienciación.

Equipo de TI y Seguridad

- **Responsabilidades:** Proporcionar apoyo técnico para las sesiones de capacitación y asistir en la creación de materiales educativos, como guías de mejores prácticas y manuales de respuesta a incidentes.

Evaluación y Mejora Continua

1. **Evaluaciones de Conocimientos:** Al final de cada sesión de capacitación anual, los empleados deben completar una breve evaluación de conocimientos para verificar la comprensión de los temas clave.
2. **Encuestas de Satisfacción:** Después de cada capacitación, los empleados recibirán una encuesta para evaluar la calidad de la capacitación y sugerir mejoras.
3. **Actualización de Materiales:** Cada seis meses, el Coordinador de Capacitación revisará los materiales y actualizará el contenido de acuerdo con las nuevas amenazas y mejores prácticas de seguridad.

Este plan de concienciación y capacitación en seguridad garantiza que todos los empleados de UCOP estén informados y comprometidos con la protección de la información. A través de sesiones de capacitación periódicas y materiales de apoyo, UCOP busca fomentar una cultura de seguridad que minimice los riesgos de ciberseguridad y mejore la respuesta a incidentes.

Política de Aprobación y Revisión de Documentos de Seguridad en UCOP

La aprobación y revisión regular de las políticas y procedimientos de seguridad son esenciales para garantizar que se mantengan actualizadas y efectivas frente a las amenazas y cambios regulatorios. Esta política establece el proceso de aprobación y un cronograma de revisiones periódicas para asegurar el cumplimiento continuo y la adecuación de las políticas de seguridad en UCOP.

1. Aprobación de Políticas y Procedimientos

A. Proceso de Aprobación

1. **Creación o Modificación de Documentos:** Todos los documentos de políticas y procedimientos de seguridad deben ser creados o revisados por el equipo de seguridad de TI y elaborados con la colaboración de las áreas implicadas.
2. **Revisión Interna:** Una vez preparados, los documentos deben pasar una revisión interna en el equipo de seguridad para garantizar su coherencia y conformidad con los estándares de UCOP.
3. **Presentación a la Dirección Ejecutiva:** Los documentos revisados internamente serán presentados a la dirección ejecutiva de UCOP para su revisión final y aprobación.
4. **Aprobación Formal:** La dirección ejecutiva debe aprobar formalmente los documentos antes de que sean implementados, asegurando su alineación con los objetivos y valores de la organización.

B. Registro de Aprobación

Cada documento aprobado debe incluir una sección de firma y fecha de aprobación, indicando los nombres y roles de las personas que autorizaron el documento. Los documentos deben ser registrados en el sistema de gestión de documentos de UCOP para su control y acceso.

2. Cronograma de Revisión y Actualización de Documentos

A. Revisión Anual de Políticas de Seguridad

- **Frecuencia:** Anualmente.
- **Objetivo:** Asegurar que las políticas de seguridad continúan alineadas con las mejores prácticas, normativas aplicables (como FERPA y HIPAA), y responden a los cambios en el entorno de amenazas.
- **Responsable:** Equipo de Seguridad de TI, en coordinación con el Departamento de Cumplimiento.
- **Proceso:** Revisión completa de los documentos, actualizando cualquier sección que requiera ajustes y sometiendo los cambios a aprobación de la dirección ejecutiva.

B. Revisión Trimestral de Procedimientos Críticos

- **Frecuencia:** Trimestralmente.
- **Objetivo:** Revisar procedimientos específicos que son críticos para la seguridad operativa, como el control de acceso, la respuesta a incidentes y las copias de seguridad.
- **Responsable:** Equipo de Seguridad de TI y supervisores de áreas específicas.
- **Proceso:** Revisar la efectividad de los procedimientos y hacer ajustes menores si es necesario. Cualquier cambio significativo debe ser aprobado por la dirección ejecutiva.

C. Actualización por Cambios Regulatorios o Amenazas Emergentes

- **Frecuencia:** Según sea necesario.
- **Objetivo:** Ajustar las políticas y procedimientos en respuesta a cambios regulatorios, nuevas amenazas o incidentes significativos.
- **Responsable:** Equipo de Seguridad de TI y Departamento de Cumplimiento.
- **Proceso:** Cuando se identifique un cambio crítico en el entorno de seguridad o en la normativa, se revisará y actualizará la política o procedimiento relevante, obteniendo la aprobación formal para su implementación inmediata.

---

3. Seguimiento y Control de Versiones

- **Historial de Revisiones:** Cada documento debe incluir un historial de revisiones, donde se registre cada actualización con fecha, cambios realizados y nombre del responsable.
- **Control de Versiones:** Se establecerá un sistema de control de versiones que facilite la identificación de la versión actual de cada documento, evitando el uso de documentos desactualizados.
- **Almacenamiento y Acceso:** Los documentos de políticas y procedimientos se almacenarán en el sistema de gestión de documentos de UCOP, con acceso controlado para garantizar que solo el personal autorizado pueda consultarlos y editarlos.

El proceso de aprobación y el cronograma de revisiones periódicas aseguran que las políticas y procedimientos de UCOP se mantengan actualizados y efectivos frente a los cambios en el entorno de amenazas y las normativas aplicables. Este enfoque sistemático fortalece la capacidad de UCOP para responder a nuevos desafíos de seguridad,

manteniendo un compromiso continuo con la protección de la información y la mejora continua de su sistema de gestión de seguridad.

Conclusión General del Sistema de Gestión de Seguridad de la Información (SGSI) de UCOP

El Sistema de Gestión de Seguridad de la Información (SGSI) de la University of California Office of the President (UCOP) constituye una estructura integral y adaptativa diseñada para proteger los activos de información críticos de la organización frente a amenazas internas y externas. Este sistema se alinea con estándares reconocidos, como **ISO/IEC 27001**, **NIST**, y **CIS**, y responde a las regulaciones aplicables, incluidas **FERPA** y **HIPAA**, proporcionando un marco sólido de cumplimiento y seguridad. A lo largo de su diseño e implementación, el SGSI ha integrado políticas, procedimientos, controles y prácticas de seguridad robustos que no solo protegen la confidencialidad, integridad y disponibilidad de la información, sino que también fomentan una cultura de seguridad continua dentro de UCOP.

Uno de los pilares fundamentales del SGSI es su enfoque en la **gestión de riesgos**. Este proceso permitió identificar activos críticos, evaluar las amenazas y vulnerabilidades a las que están expuestos, y priorizar los riesgos en función de su probabilidad e impacto. Esta priorización de riesgos ha guiado la implementación de controles específicos, como firewalls de próxima generación (NGFW), autenticación multifactor (MFA), cifrado de datos sensibles, sistemas de detección y prevención de intrusos (IDPS), y un sistema de copias de seguridad y recuperación de datos, todos diseñados para mitigar las amenazas más apremiantes. Estos controles también son viables y sostenibles en un entorno de recursos públicos como UCOP, lo que asegura su efectividad a largo plazo.

La **gestión de accesos** es otro componente clave del SGSI, garantizando que solo los usuarios autorizados accedan a la información y los sistemas críticos. El Control de Acceso

Basado en Roles (RBAC), en conjunto con políticas de contraseñas seguras y autenticación multifactor, asegura que los permisos de acceso se concedan y mantengan de acuerdo con las responsabilidades y necesidades de cada usuario. Esto, junto con las auditorías de acceso y la capacitación en el manejo seguro de contraseñas, protege los sistemas contra accesos no autorizados y minimiza el riesgo de exposición de datos.

Además, el **Plan de Respuesta a Incidentes** del SGSI establece procedimientos claros para la identificación, contención, erradicación y recuperación ante incidentes de seguridad. Este plan incluye roles y responsabilidades definidos para el Equipo de Respuesta a Incidentes (IRT) y otros departamentos, lo que permite una respuesta rápida y efectiva ante posibles eventos de seguridad, minimizando el impacto en las operaciones de UCOP y fortaleciendo la resiliencia organizacional.

La **capacitación y concienciación en seguridad** de los empleados es fundamental para la implementación efectiva del SGSI. A través de programas de formación continua y materiales de concienciación, como carteles y guías de buenas prácticas, UCOP promueve una cultura de seguridad que involucra a todos los empleados en la protección de la información. Esta educación continua permite que los empleados reconozcan y respondan a amenazas potenciales, como correos electrónicos de phishing, contribuyendo activamente a la seguridad de la organización.

Finalmente, la **revisión y mejora continua** son esenciales para mantener la relevancia y efectividad del SGSI de UCOP. La política de aprobación y revisión de documentos garantiza que todas las políticas y procedimientos sean revisados anualmente, con revisiones adicionales en respuesta a cambios regulatorios o incidentes de seguridad significativos. Este enfoque asegura que el SGSI esté alineado con las mejores prácticas y las nuevas amenazas, permitiendo a UCOP adaptarse a los cambios del entorno de ciberseguridad y cumplir con los requisitos normativos vigentes.

En conclusión, el SGSI de UCOP establece un enfoque estructurado y proactivo para proteger los activos de información críticos, asegurar la continuidad operativa y promover una cultura de seguridad en toda la organización. La implementación de controles de seguridad eficaces, la capacitación del personal y el compromiso con la mejora continua refuerzan la posición de UCOP en el cumplimiento de sus objetivos de seguridad y su responsabilidad de proteger la información confiada por estudiantes, empleados y otros actores relevantes.