Informe Nº 0001 - 2024/UNSM-JLKV

Título: Evaluación del Sistema de Inscripción en la Oficina de Admisión de la UNSM.

Empresa Auditora: Anónimo S.A.C

Jeysond Atamirano Vega
Firmado digitalmente por Jeysond Atamirano Vega
Fecha: 2024.07.02 13:28:43 -05'00'

Luis Carlos Arevalo Ocampo
Firmado digitalmente por Luis Carlos Arevalo Ocampo
Fecha: 2024.07.02 13:29:08 -05'00'

karen Alely Chamaya Guevara
Firmado digitalmente por karen Alely Chamaya Guevara
Fecha: 2024.07.02 13:29:38 -05'00'

Victor Hugo Bravo Garcia
Firmado digitalmente por Victor Hugo Bravo Garcia
Fecha: 2024.07.02 13:30:03 -05'00'

Auditores responsables:

Jeysond Altamirano Vega

Luis Carlos Arevalo Ocampo

Victor Hugo Bravo Garcia

Karen Alely Chamaya Guevara

Fecha de corte: 20/03/2024

Periodo: 2024 - I

Fecha de Entrega: 02/07/2024

1.- Introducción

El avance tecnológico actual ha aportado numerosos beneficios a las empresas, facilitando un crecimiento significativo en los procesos que los clientes exigen. Sin embargo, estos avances también han incrementado los riesgos a los que se enfrentan las organizaciones, amenazando el cumplimiento de su misión y objetivos institucionales. En este contexto, la administración de riesgos emerge como una disciplina crucial que proporciona los medios necesarios para identificar, medir y responder adecuadamente a los riesgos, protegiendo los intereses, el patrimonio y la responsabilidad de la organización.

Para hacer frente a estos riesgos, es fundamental llevar a cabo un análisis exhaustivo. Este análisis permite a las empresas e instituciones identificar los activos que poseen y las vulnerabilidades que pueden enfrentar tanto desde factores externos como internos, los cuales podrían afectar sus intereses y su patrimonio. Además, proporciona las bases para la elaboración de políticas de seguridad y directrices claras que deben cumplir todos los miembros del personal de la organización, asegurando así una gestión efectiva de los riesgos.

El enfoque planteado en este trabajo se orienta hacia la realización de un estudio exhaustivo en la dirección de Admisión de la Universidad Nacional de San Martín (UNSM), con el objetivo de identificar la situación actual de cómo se encuentra, proponer medidas de mitigación y abordar los riesgos de forma progresiva. Este análisis se enfocará especialmente en la gestión de riesgos dentro de la dirección de admisión de la UNSM, con el fin de asegurar la continuidad y eficiencia de sus operaciones.

2.- Objetivo de la actividad de control

Evaluar los activos y riesgos asociados con la dirección de Admisión de la Universidad Nacional de San Martín (UNSM) para identificar la situación actual de la gestión de riesgos, proponer medidas de mitigación efectivas y desarrollar estrategias que aseguren la integridad, disponibilidad y confidencialidad de los procesos y sistemas utilizados, garantizando así la continuidad y eficiencia operativa de la institución y la protección de sus intereses y patrimonio.

Objetivos Específicos

- Inspeccionar y analizar los activos tecnológicos de la dirección de Admisión de la UNSM para identificar vulnerabilidades y amenazas que comprometan la integridad, disponibilidad y confidencialidad de los procesos y sistemas.
- Sugerir medidas de mitigación efectivas para resolver los problemas identificados durante la evaluación de riesgos, optimizando la gestión de riesgos de manera proactiva.
- Evaluar exhaustivamente los riesgos asociados con los procesos y sistemas de la dirección de Admisión, identificando puntos críticos y áreas de mejora.

Objetivos Estratégicos Institucionales de la UNSM

La UNSM cuenta con cinco (5) objetivos estratégicos en su Plan Estratégico Institucional 2020-2023, los cuales se listan a continuación:

- OEI 1. Mejorar la calidad de la formación académica y profesional de los estudiantes universitarios.
- OEI 2. Promover la investigación y el emprendimiento en la comunidad universitaria.
- OEI 3. Fomentar actividades de extensión cultural y proyección social en la comunidad universitaria.
- OEI 4. Fortalecer la gestión institucional.
- OEI 5. Implementar la gestión de riesgo ante desastres.ç

3.- Alcance

El objetivo es identificar y evaluar los riesgos y amenazas a los que está expuesta esta oficina, con el fin de cuantificarlos y proponer salvaguardas para mitigarlos a niveles mínimos. De esta manera, se busca mejorar la protección de la información y de los activos que la contienen, garantizando la continuidad y seguridad de los procesos de admisión en la UNSM.

El análisis abarca todas las etapas del proceso de admisión. Primero, en la **Etapa de Inscripción**, se evaluarán los riesgos asociados con la inscripción de los postulantes, incluyendo la recopilación y almacenamiento seguro de los datos personales.

En la **Etapa de Evaluación**, se abordarán los exámenes ordinarios y extraordinarios. Se analizarán los riesgos durante la administración de ambos tipos de exámenes, asegurando la integridad y confidencialidad de las pruebas, y teniendo en cuenta las diferentes modalidades de postulación.

Finalmente, en la **Etapa Post Examen**, se evaluarán los riesgos relacionados con el manejo y almacenamiento de los resultados de los exámenes, así como la comunicación de los mismos a los postulantes.

A través de este enfoque, se pretende asegurar que cada etapa del proceso de admisión esté adecuadamente protegida contra posibles amenazas, garantizando la integridad, disponibilidad y confidencialidad de la información y de los procesos involucrados.

4.- Antecedentes

El análisis de riesgos en la oficina de Admisión de la Universidad Nacional de San Martín (UNSM) se fundamenta en auditorías previas realizadas en universidades peruanas. En la Universidad Nacional Mayor de San Marcos (UNMSM) y la Escuela Nacional de Control (ENC), se han implementado maestrías en auditoría gubernamental, enfocadas en la evaluación de políticas públicas y auditorías presupuestales. Estos programas han demostrado ser efectivos en mantener la transparencia y confianza en las instituciones académicas.

La Universidad Nacional Federico Villarreal (UNFV) ha llevado a cabo investigaciones significativas en auditoría interna aplicada a universidades. Las tesis desarrolladas en la Facultad de Ciencias Financieras y Contables destacan la importancia de un control interno eficiente para el buen gobierno de las entidades públicas. Estos estudios proporcionan un marco teórico robusto para entender cómo la auditoría interna puede optimizar la gestión institucional en universidades.

En la Universidad Nacional de San Agustín (UNSA), se han realizado trabajos sobre auditoría académica y control administrativo que resaltan la necesidad de auditar tanto las transacciones financieras como los aspectos académicos y administrativos. La implementación de auditorías académicas ha sido crucial para mejorar la gestión y asegurar el cumplimiento de las metas y objetivos institucionales. Estos antecedentes subrayan la relevancia de auditorías exhaustivas en universidades peruanas, enfocándose en la gestión académica y administrativa para asegurar una administración eficiente y transparente.

5.- Base legal

- Ley Universitaria (Ley N° 30220)
- ISO/IEC 27001:2013 - Sistema de Gestión de Seguridad de la Información (SGSI)
- ISO 31000: Gestión del riesgo – Principios y directrices.
- ISO 9001: Sistemas de gestión de la calidad.
- COSO (Committee of Sponsoring Organizations of the Treadway Commission): Marco integrado de control interno ampliamente aceptado.
- Ley N° 29783: Ley de Seguridad y Salud en el Trabajo.
- NIST SP 800-53 - Controles de Seguridad y Privacidad para Sistemas de Información Federales y Organizaciones

6.- Observaciones

- Gestión de contraseñas y acceso a sistemas: Se identificó una falta de políticas especializadas que aborden aspectos clave de seguridad, como la gestión de contraseñas, el acceso a sistemas y el uso de dispositivos personales. La ausencia de estas políticas puede aumentar el riesgo de accesos no autorizados y comprometer la seguridad de los recursos informáticos
- Mecanismos de autenticación: Actualmente, los mecanismos de autenticación en uso no son suficientemente robustos. La falta de autenticación de dos factores o biométrica para proteger el acceso a los sistemas y la información confidencial puede exponer a la universidad a riesgos significativos de seguridad.
- Plan de respuesta a incidentes: No se ha desarrollado ni implementado un plan de respuesta a incidentes adecuado. La ausencia de procedimientos establecidos para responder a brechas de seguridad, ataques cibernéticos u otros incidentes puede llevar a una respuesta lenta e ineficaz ante situaciones de crisis.
- Backup y recuperación de datos: Se detectó que no se cuenta con sistemas de backup automatizados confiables. La falta de copias de seguridad regulares y seguras compromete la capacidad de la universidad para recuperar información crítica en caso de pérdida de datos.
- Capacitación en manejo de datos: Se observó que el personal de la Oficina de Admisión no ha recibido capacitación adecuada en prácticas seguras de manejo de datos. La falta de formación puede resultar en la manipulación incorrecta de datos y aumentar el riesgo de pérdida de información crítica.
- Procedimientos para recepción y almacenamiento de documentos: Se carece de procedimientos claros y documentados para la recepción, revisión y almacenamiento de los documentos de los postulantes. Esto puede resultar en inconsistencias y errores durante el proceso de admisión.
- Identificación de postulantes durante la orientación: Las políticas para la identificación de los postulantes durante la orientación no son lo suficientemente estrictas. La falta de verificación adecuada de documentos de identificación oficiales puede permitir la suplantación de identidad.
- Pruebas de carga y estrés en sistemas: No se realizan pruebas de carga y estrés periódicas para evaluar la capacidad de los sistemas de manejar picos de tráfico durante el proceso de inscripción. Esto puede llevar a interrupciones en el servicio y afectaciones eAutenticación y autorización en el sistema de puntaje de resultados: Los mecanismos de autenticación y autorización para el acceso al sistema de puntaje de

resultados no son robustos, lo que podría permitir el acceso y manipulación de información por personal no autorizado.n la calidad del proceso de admisión.

- Protocolos de transporte seguro para exámenes: Los protocolos de transporte y medidas de seguridad para proteger la información sensible durante el transporte del personal docente no son suficientes. La falta de control y monitoreo adecuados puede resultar en la revelación no autorizada de información crítica.

7.- Recomendaciones

- Capacitar al personal de la Oficina de Admisión en prácticas seguras de manejo de datos. La formación debe incluir la sensibilización sobre las consecuencias de la pérdida de datos y las medidas preventivas que deben tomarse, en línea con la Ley de Seguridad y Salud en el Trabajo (Ley N° 29783).
- Establecer un proceso continuo de monitoreo y evaluación de la información contenida en los prospectos y otros documentos críticos. Esto ayudará a identificar y mitigar riesgos de alteración de datos de manera proactiva, conforme a la ISO 31000.
- Para asegurar la continuidad operativa y la integridad de los datos, se recomienda la implementación de servicios de backup automatizados. Estos sistemas deben realizar copias de seguridad regulares y seguras, alineadas con la normativa ISO 27001.
- Desarrollar políticas y programas que promuevan la responsabilidad y el cumplimiento de las normas de seguridad entre todos los miembros de la universidad. Esto incluye la capacitación regular y la concientización sobre las mejores prácticas de seguridad.
- Se debe tener un plan detallado para responder a incidentes de seguridad. Este plan debe incluir procedimientos para manejar brechas de seguridad, ataques cibernéticos y otros incidentes relacionados, asegurando una respuesta rápida y efectiva para minimizar los daños y restaurar la normalidad lo antes posible
- Desarrollar y documentar procedimientos claros para la recepción, revisión y almacenamiento de documentos de los postulantes. Asegurar que estos procedimientos sean seguidos estrictamente y estén alineados con el marco de control interno COSO.
- Adoptar un Sistema de Gestión de Seguridad de la Información (SGSI),basado en la norma ISO 27001, para proteger la confidencialidad, integridad y disponibilidad de la información confidencial de los postulantes. Este sistema debe incluir políticas, procedimientos y controles técnicos adecuados.
- Realizar pruebas periódicas de carga y estrés para identificar los límites del sistema y asegurar que puede manejar picos de tráfico durante el proceso de inscripción. Estas pruebas deben seguir las recomendaciones de la ISO 9001 para asegurar la calidad del servicio.
- Mejorar continuamente las estrategias y tecnologías de mitigación de ataques DDoS. Las medidas adoptadas deben estar conforme a las normas ISO 27001 e ISO 31000 para la gestión de seguridad de la información y riesgos.
- Implementar un proceso de revisión y aprobación para todas las publicaciones de información. Asegurar que todas las modificaciones sean revisadas y aprobadas por múltiples niveles jerárquicos antes de ser publicadas.
- Configurar controles de acceso estrictos y permisos basados en roles para limitar quién puede eliminar o modificar información publicada. Solo el personal autorizado debe tener la capacidad de eliminar información crítica.
- Establecer un programa riguroso de actualización y parcheo del software, incluyendo SIGAU y SGD. Asegurarse de que todos los componentes del software estén siempre

actualizados con los últimos parches de seguridad, siguiendo las mejores prácticas de la ISO 27001.

- Capacitar al personal técnico en las mejores prácticas de mantenimiento y actualización de software, incluyendo la identificación y corrección de errores comunes y la implementación segura de cambios. Esta capacitación debe alinearse con las directrices de la ISO 27001.
- Implementar cifrado fuerte para todos los datos biométricos almacenados y transmitidos por el sistema de registro de huellas. Asegurarse de que las claves de cifrado estén protegidas adecuadamente y que el acceso a ellas esté restringido.
- Establecer mecanismos de autenticación y autorización robustos para el acceso al sistema de puntaje de resultados. Utilizar autenticación multifactor (MFA) y control de acceso basado en roles (RBAC) para limitar el acceso a información sensible y funciones críticas.
- Implementar una política estricta que prohíba el uso de dispositivos móviles por parte del personal de apoyo durante los exámenes. Utilizar alternativas como walkie-talkies para la comunicación interna y establecer controles para asegurar el cumplimiento de esta normativa.
- Establecer protocolos de transporte y medidas de seguridad estrictas para proteger la información sensible durante el transporte del personal docente que crea el examen de admisión ordinario. Implementar sistemas de comunicación segura y monitoreo en tiempo real durante el transporte.

8.- Conclusiones

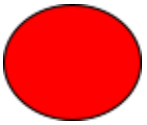
La evaluación de riesgos en la dirección de Admisión de la Universidad Nacional de San Martín (UNSM) ha revelado múltiples áreas críticas que requieren atención inmediata para garantizar la seguridad de la información y la continuidad operativa. La falta de políticas especializadas, mecanismos de autenticación robustos y una cultura sólida de seguridad informática expone a la universidad a riesgos significativos que pueden comprometer la integridad, disponibilidad y confidencialidad de sus procesos y sistemas. Además, la ausencia de un plan de respuesta a incidentes y de sistemas de backup automatizados pone en peligro la capacidad de recuperación ante eventos adversos.

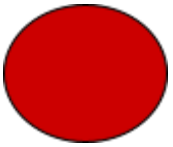
Es fundamental que la UNSM adopte un enfoque proactivo en la gestión de riesgos, implementando las recomendaciones propuestas, que incluyen la simplificación de procesos burocráticos, el establecimiento de controles de acceso estrictos y la capacitación del personal en prácticas seguras. Estas medidas no solo mejorarán la seguridad de los activos tecnológicos y la información sensible, sino que también fortalecerán la confianza en la institución y garantizarán la eficiencia y efectividad de sus operaciones. Al adoptar estándares internacionales como ISO 27001 e ISO 31000, la UNSM podrá crear un entorno seguro y resiliente, preparado para enfrentar los desafíos actuales y futuros.

Area: TI

<table>
<tr><td colspan="2">Proceso:</td><td>Área: Oficina de admisión</td><td>Nivel de riesgo</td></tr>
<tr><td>Nº</td><td>Hallazgo</td><td>Riesgo Potencial</td><td></td></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Se identificó un riesgo de revelación no autorizada de la información sobre la ubicación exacta de los postulantes durante el proceso de asignación de aulas. Esta información es conocida únicamente por una persona y almacenada en una computadora sin acceso a internet para mayor seguridad. Sin embargo, la centralización del conocimiento en una sola persona y la falta de acceso controlado pueden llevar a la vulnerabilidad de la información. Esta situación podría comprometer la confidencialidad de la información y la integridad del proceso de admisión.</td><td>Existe el riesgo de la suplantación de la identidad del postulante.
Al filtrar la información acerca de la ubicación de los postulantes se puede colocar una posible ficha de respuestas para el examen.</td><td>  </td></tr>
<tr><td colspan="2">RECOMENDACIÓN</td></tr>
<tr><td colspan="2">Implementar métodos de autenticación multifactor (MFA) utilizando más de un método de verificación de identidad, como contraseñas, tokens físicos y biometría (huellas digitales, reconocimiento facial). La sección relevante que aborda la autenticación y el control de acceso es la norma ISO/IEC 27001:2013. Esto ayuda a controlar y mejorar la seguridad en relación con el riesgo de suplantación de identidad del postulante y el uso indebido de la información de ubicación.</td></tr>
</table>

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Durante la revisión observamos que existe un riesgo significativo de información sensible durante la preparación y supervisión del examen. Los docentes que elaboran el examen, tienen acceso a información crítica, lo que incrementa la posibilidad de divulgación no autorizada. Aunque se han implementado medidas de seguridad como el almacenamiento de información en computadoras sin acceso a internet y la requisición de dispositivos electrónicos, la participación de varias personas en el manejo de información crítica sigue siendo una vulnerabilidad considerable.	• Un docente podría ser sobornado o presionado por terceros, como familiares de los postulantes, para revelar información del examen a cambio de una compensación económica o favores. • La falta de capacitación adecuada en seguridad de la información puede llevar a que los docentes no comprendan la gravedad de las medidas de seguridad, resultando en un manejo descuidado de la información crítica.	
		RECOMENDACIÓN	
		Se recomienda implementar sistemas de monitoreo y control de acceso para limitar y registrar quién tiene acceso a la información del examen y en qué momentos. Esto puede incluir el uso de sistemas de autenticación multifactor y la asignación de permisos basados en roles para asegurar que solo el personal autorizado pueda acceder a información crítica. Los registros de acceso deben ser auditados regularmente para detectar cualquier actividad sospechosa. Esto está relacionado con los controles A.9.4.2 y A.9.1.2 de la norma ISO/IEC 27001:2013, que mencionan los sistemas de monitoreo y control de accesos, junto con la autenticación multifactor y la gestión de permisos basados en roles.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Durante la revisión observamos que existe un riesgo significativo de filtración de información importante del examen durante el transporte del personal docente que crea el examen de admisión ordinario. La vigilancia de los docentes es realizada únicamente por la comisión, la cual viaja en una camioneta separada. Esta falta de control y supervisión directa durante el transporte puede resultar en la revelación no autorizada de información sensible del examen, comprometiendo la integridad del proceso de admisión.	• La separación física entre la comisión y los docentes durante el transporte reduce la capacidad de monitorear de cerca las actividades de los docentes y responder rápidamente a cualquier incidente sospechoso.	
		RECOMENDACIÓN	
		Es crucial implementar medidas adicionales para proteger la información sensible durante el transporte del personal docente que crea el examen de admisión ordinario y limitar el acceso no autorizado. Esto incluye establecer protocolos de transporte y medidas de seguridad estrictas basadas en normativas de seguridad de la información como la ISO/IEC 27001, así como otras bases legales aplicables en el ámbito educativo y de protección de datos. Se recomienda que la comisión viaje en el mismo vehículo que los docentes para mantener un control directo y continuo. Además, es fundamental implementar sistemas de comunicación segura y monitoreo en tiempo real durante el transporte para detectar y prevenir cualquier intento de divulgación no autorizada de la información.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificó un riesgo relacionado con el personal de apoyo que asiste durante los exámenes, quienes portan sus celulares mientras realizan la verificación de huellas dactilares en las aulas. Esta práctica, además de incomodar a los postulantes, está prohibida y puede comprometer la integridad del proceso de admisión.	● La presencia de dispositivos móviles en las aulas durante la verificación de huellas dactilares puede facilitar la filtración de información, comprometer la confidencialidad del examen y generar incomodidad en los postulantes.	
		RECOMENDACIÓN	
		Implementar una política estricta que prohíba el uso de dispositivos móviles por parte del personal de apoyo durante los exámenes. Se recomienda el uso de walkie-talkies para la comunicación interna y establecer controles para asegurar el cumplimiento de esta normativa, conforme a las directrices de la ISO/IEC 27001. Esto se alinea con los controles A.6.2.1 (Política de uso aceptable), A.9.2.3 (Gestión de acceso privilegiado), A.11.2.6 (Seguridad en las áreas de trabajo), A.12.4.1 (Registro de eventos) y A.13.1.1 (Políticas y procedimientos para la gestión de la comunicación), asegurando así la integridad del proceso de examen, el control del uso de dispositivos y la implementación de comunicaciones seguras.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
01	La Oficina de Admisión no cuenta con una política, procedimiento y lineamientos claros para la protección y retención de información crítica en los reportes institucionales. Observamos que no existen medidas de seguridad adecuadas, como sistemas de respaldo y redundancia en el almacenamiento de datos, lo cual incrementa el riesgo de que la información crítica sea destruida accidentalmente o intencionalmente.	La destrucción no controlada de información crítica en reportes institucionales puede dar lugar a la pérdida de datos esenciales para la operación y la toma de decisiones. Esto puede afectar negativamente la transparencia y la integridad de los procesos administrativos, comprometiendo la capacidad de la Oficina de Admisión para cumplir con sus objetivos operativos y estratégicos. La pérdida de información crítica puede resultar en decisiones mal informadas, retrasos en los procesos y una disminución de la confianza en la gestión de la información.	

		RECOMENDACIÓN
		Es conveniente establecer reglas y directrices claras relacionadas con la protección y retención de información crítica en los reportes institucionales, alineadas con la norma ISO/IEC 27001:2013, que especifica la necesidad de implementar controles y medidas de seguridad adecuadas para la gestión de información. Se deben establecer y aplicar políticas que rijan la retención y protección de datos críticos, asegurando la implementación de sistemas de respaldo y redundancia en el almacenamiento de datos.

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
2.1	La Oficina de Admisión no cuenta con controles adecuados para evitar la alteración de la información en los documentos presentados por los postulantes. Observamos que no existen procedimientos de verificación robustos ni sistemas de auditoría que aseguren la integridad de los documentos durante el proceso de revisión y validación.	Existe el riesgo de que los documentos presentados sean alterados, comprometiendo la integridad del proceso de revisión y validación. La alteración de la información puede llevar a decisiones erróneas, admisiones incorrectas y pérdida de confianza en el proceso de selección, afectando negativamente la reputación y la eficiencia operativa de la Oficina de Admisión.	
		RECOMENDACIÓN	
		• Es conveniente establecer controles de verificación de documentos y sistemas de auditoría alineados con la norma NTP-ISO/IEC 27001:2014, que especifica la necesidad de implementar medidas de seguridad adecuadas para proteger la integridad de la información. Se deben definir y aplicar políticas claras que rijan la verificación de documentos, asegurando que cada documento presentado sea validado y auditado sistemáticamente • El área de TI debe implementar un sistema de verificación que utilice tecnologías avanzadas, como la autenticación digital y el sellado de tiempo, para asegurar que los documentos no sean alterados después de su presentación. Además, se deben establecer procedimientos de auditoría regulares para revisar y validar la integridad de los documentos de manera continua.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
2.2	La Oficina de Admisión no cuenta con controles adecuados para prevenir el acceso no autorizado a la información confidencial de los postulantes. Observamos que no se han implementado medidas de seguridad como la autenticación de dos factores y los controles de acceso basados en roles, lo cual incrementa el riesgo de que personas no autorizadas accedan a la información confidencial.	Existe el riesgo de que personas no autorizadas accedan a los documentos, comprometiendo la confidencialidad de la información. El acceso no autorizado puede llevar a la exposición de datos sensibles, pérdida de confianza por parte de los postulantes y posibles incumplimientos de las normativas de protección de datos.	
		RECOMENDACIÓN	
		• Es conveniente implementar autenticación de dos factores (2FA) y controles de acceso basados en roles (RBAC) alineados con la norma NTP-ISO/IEC 27001:2014, que especifica la necesidad de implementar medidas de seguridad adecuadas para proteger la confidencialidad de la información. Se deben establecer y aplicar políticas claras que rijan el acceso a la información confidencial, asegurando que solo el personal autorizado tenga acceso a los datos sensibles. • Es importante capacitar al personal en las mejores prácticas de seguridad de la información, incluyendo el uso de autenticación de dos factores y la importancia de los controles de acceso. Asegurarse de que todos los empleados comprendan la importancia de la confidencialidad de la información y su rol en la protección de los datos de los postulantes.	

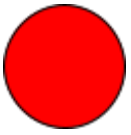
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
3	La Oficina de Admisión no cuenta con controles adecuados para prevenir la suplantación de identidad durante el proceso de orientación a los postulantes. Observamos que no existen verificaciones rigurosas de identidad ni procedimientos establecidos para la detección de suplantación de identidad.	Existe el riesgo de que se suplante la identidad de orientadores o postulantes durante la orientación, afectando la veracidad de la información proporcionada. La suplantación de identidad puede llevar a la provisión de información incorrecta o fraudulenta, lo cual compromete la integridad y confianza en el proceso de orientación y admisión.	
		RECOMENDACIÓN	
		Es importante capacitar al personal encargado de la orientación en las mejores prácticas de verificación de identidad y en la detección de posibles intentos de suplantación. Asegurarse de que comprendan la importancia de la integridad de la identidad en el proceso de orientación y su rol en la protección contra la suplantación alineacineadose a la norma ISO/IEC 27001:2013,	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
4	El sistema de inscripción no cuenta con medidas adecuadas para manejar la carga alta durante los períodos de inscripción, lo que puede resultar en caídas del sistema debido al agotamiento de recursos. Observamos que no se han implementado soluciones de escalabilidad automática ni se realizan pruebas de capacidad antes de los períodos críticos de inscripción.	Existe el riesgo de que el sistema experimente caídas debido a una carga inesperadamente alta durante las inscripciones, lo cual interrumpiría el proceso de inscripción y afectaría negativamente la experiencia de los postulantes y la eficiencia operativa de la Oficina de Admisión.	
		RECOMENDACIÓN	
		Es recomendable implementar soluciones de escalabilidad automática y realizar pruebas de capacidad antes de los períodos críticos de inscripción, alineadas con la norma ISO/IEC 27001:2013 y la norma ISO 22301:2019 de gestión de la continuidad del negocio.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
06.1	Se identificó un riesgo considerable de uso indebido de la orientación para propósitos no autorizados, comprometiendo la efectividad del proceso de admisión.	Uso indebido de la orientación para propósitos no autorizados	
		RECOMENDACIÓN	
		Capacitar al personal encargado de la orientación en las políticas y procedimientos establecidos, y en la identificación y prevención del uso indebido de la orientación. La capacitación debe enfatizar la importancia de adherirse a los propósitos autorizados y las consecuencias del incumplimiento.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
07.1	Se identificó un riesgo significativo de interrupción del proceso de inscripción debido a caídas del sistema, causadas por una carga inesperadamente alta durante las inscripciones	Interrupción del proceso de inscripción debido a caídas del sistema	
		RECOMENDACIÓN	
		Realizar pruebas de carga y estrés periódicas para identificar los límites del sistema y asegurar que puede manejar picos de tráfico durante el proceso de inscripción. Estas pruebas deben seguir las recomendaciones de la ISO 9001 para asegurar la calidad del servicio.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
07.2	Se identificó un riesgo considerable de que el sistema sea objeto de un ataque de denegación de servicio (DDoS) durante las inscripciones, afectando su disponibilidad y rendimiento.	El ataque de denegación de servicio afecta la disponibilidad del sistema.	
		RECOMENDACIÓN	
		Revisar y mejorar continuamente las estrategias y tecnologías de mitigación de DDoS para adaptarse a nuevas tácticas de ataque y tecnologías emergentes, conforme a las normas ISO 27001 e ISO 31000 para la gestión de seguridad de la información y riesgos.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
08.1	Se identificó un riesgo significativo de modificación de la información publicada, lo cual puede causar desinformación y confusión entre los postulantes.	Modificación de la información publicada, causando desinformación.	
		RECOMENDACIÓN	
		Implementar un proceso de revisión y aprobación para todas las publicaciones de información. Asegurar que todas las modificaciones sean revisadas y aprobadas por múltiples niveles jerárquicos antes de ser publicadas.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
08.2	Se identificó un riesgo considerable de eliminación accidental o intencional de información crítica publicada, afectando la transparencia del proceso de admisión.	Eliminación accidental o intencional de información crítica publicada.	
		RECOMENDACIÓN	
		Configurar controles de acceso estrictos y permisos basados en roles (RBAC) para limitar quién puede eliminar información publicada. Solo el personal autorizado debe tener la capacidad de eliminar o modificar información crítica.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
09.1	Se identificó un riesgo significativo de exposición a vulnerabilidades en el software del SIGAU, que podrían ser explotadas por atacantes.	Exposición a vulnerabilidades que podrían ser explotadas.	
		RECOMENDACIÓN	
		Establecer un programa riguroso de actualización y parcheo del software SIGAU. Asegurarse de que todos los componentes del software estén siempre actualizados con los últimos parches de seguridad, siguiendo las mejores prácticas de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
09.2	Se identificó un riesgo considerable de que errores durante el mantenimiento o actualización del software afecten la estabilidad y seguridad del SIGAU.	Posibilidad de errores durante el mantenimiento o actualización.	
		RECOMENDACIÓN	
		Capacitar al personal técnico en las mejores prácticas de mantenimiento y actualización de software, incluyendo la identificación y corrección de errores comunes y la implementación segura de cambios. Esta capacitación debe alinearse con las directrices de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
09.3	Se identificó un riesgo significativo de compromiso del SIGAU debido a la introducción de software malicioso.	Compromiso de la integridad y confidencialidad de los datos	
		RECOMENDACIÓN	
		Capacitar al personal en prácticas seguras de TI, incluyendo la identificación de correos electrónicos de phishing, enlaces sospechosos y la importancia de no descargar software de fuentes no confiables. Esta capacitación debe alinearse con las mejores prácticas de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
10.1	Se identificó un riesgo significativo de exposición a vulnerabilidades en el software del SGD, que podrían ser explotadas por atacantes.	Exposición a vulnerabilidades que podrían ser explotadas.	
		RECOMENDACIÓN	
		Capacitar al personal de TI y a los usuarios del SGD sobre las mejores prácticas de seguridad y la importancia de reportar cualquier anomalía o actividad sospechosa. Esta capacitación debe alinearse con las directrices de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
10.2	Se identificó un riesgo considerable de que errores durante el mantenimiento o actualización del software afecten la estabilidad y seguridad del SGD.	Posibilidad de errores durante el mantenimiento o actualización.	
		RECOMENDACIÓN	
		Capacitar al personal técnico en las mejores prácticas de mantenimiento y actualización de software, incluyendo la identificación y corrección de errores comunes y la implementación segura de cambios. Esta capacitación debe alinearse con las directrices de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
10.3	Se identificó un riesgo significativo de compromiso del SGD debido a la introducción de software malicioso.	Introducción de software malicioso.	
		RECOMENDACIÓN	
		Establecer políticas estrictas para la instalación de software en los sistemas del SGD. Solo el personal autorizado debe tener la capacidad de instalar software, y todas las instalaciones deben ser aprobadas y supervisadas por el departamento de TI.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
11	Se identificó un riesgo significativo de que el antivirus no detectara correctamente software malicioso, comprometiendo la seguridad del sistema.	El antivirus no detecta correctamente software malicioso	
		RECOMENDACIÓN	
		Realizar pruebas periódicas de eficacia del antivirus utilizando muestras de software malicioso conocidas para verificar que el antivirus detecta y maneja adecuadamente las amenazas. Estas pruebas deben ser parte de una auditoría de seguridad regular.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
12.1	Se identificó un riesgo significativo de exposición a vulnerabilidades en los sistemas operativos, que podrían ser explotadas por atacantes	Exposición a vulnerabilidades que podrían ser explotadas.	
		RECOMENDACIÓN	
		Implementar un programa riguroso de actualización y parcheo de los sistemas operativos. Asegurarse de que todos los sistemas operativos reciban las actualizaciones y parches de seguridad más recientes de manera oportuna, conforme a las mejores prácticas de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
12.2	Se identificó un riesgo considerable de que errores durante el mantenimiento o actualización del software afecten la estabilidad y seguridad de los sistemas operativos.	Posibles errores durante el mantenimiento o actualización	
		RECOMENDACIÓN	
		Capacitar al personal técnico en las mejores prácticas de mantenimiento y actualización de sistemas operativos, incluyendo la identificación y corrección de errores comunes y la implementación segura de cambios. Esta capacitación debe alinearse con las directrices de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
13.1	Se identificó un riesgo significativo de exposición a vulnerabilidades en los lectores de PDF, que podrían ser explotadas por atacantes.	Existe el riesgo de que los lectores de PDF sean vulnerables a ataques debido a vulnerabilidades en su software, lo que podría permitir a los atacantes explotar estas debilidades para comprometer la seguridad del sistema.	
		RECOMENDACIÓN	
		Evaluar y seleccionar lectores de PDF que tengan una reputación sólida en términos de seguridad y que ofrezcan características avanzadas de protección, como la capacidad de bloquear contenido sospechoso y proteger contra scripts maliciosos.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
13.2	Se identificó un riesgo considerable de que errores durante el mantenimiento o actualización del software afecten la funcionalidad de los lectores de PDF.	Existe el riesgo de que errores durante el mantenimiento o actualización del software afecten la funcionalidad de los lectores de PDF, lo que podría resultar en interrupciones del servicio y disminución de la productividad	
		RECOMENDACIÓN	
		Establecer un proceso riguroso de gestión de cambios para todas las actividades de mantenimiento y actualización de los lectores de PDF. Este proceso debe incluir la revisión y aprobación de cambios por múltiples niveles jerárquicos y la evaluación de los impactos potenciales antes de su implementación	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
14.1	Se identificó un riesgo significativo de exposición a vulnerabilidades en los editores de imágenes y videos, que podrían ser explotadas por atacantes."	Existe el riesgo de que los editores de imágenes y videos sean vulnerables a ataques debido a vulnerabilidades en su software, lo que podría permitir a los atacantes explotar estas debilidades para comprometer la seguridad del sistema.	
		RECOMENDACIÓN	
		Implementar un programa riguroso de actualización y parcheo de los editores de imágenes y videos. Asegurarse de que todas las aplicaciones reciban las actualizaciones y parches de seguridad más recientes de manera oportuna, conforme a las mejores prácticas de la ISO 27001	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
14.2	Se identificó un riesgo considerable de que errores durante el mantenimiento o actualización del software afecten la funcionalidad de los editores de imágenes y videos	Existe el riesgo de que errores durante el mantenimiento o actualización del software afecten la funcionalidad de los editores de imágenes y videos, lo que podría resultar en interrupciones del servicio y disminución de la productividad	
		RECOMENDACIÓN	
		Capacitar al personal técnico en las mejores prácticas de mantenimiento y actualización de software, incluyendo la identificación y corrección de errores comunes y la implementación segura de cambios. Esta capacitación debe alinearse con las directrices de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
15	Se identificó un riesgo significativo de pérdida de datos debido a averías lógicas en el sistema de respaldo.	Existe el riesgo de que el sistema de respaldo experimente averías lógicas, comprometiendo la integridad de los datos respaldados, lo cual podría resultar en la pérdida de información crítica y afectar la continuidad operativa	
		RECOMENDACIÓN	
		Desarrollar e implementar políticas de respaldo que incluyan copias de seguridad regulares y automáticas de todos los datos críticos. Asegurarse de que estas políticas se adhieran a las mejores prácticas y normativas como la ISO 27001	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
16.1	Se identificó un riesgo significativo de exposición a vulnerabilidades en la aplicación de Python, que podrían ser explotadas por atacantes.	Existe el riesgo de que la aplicación de Python sea vulnerable a ataques debido a vulnerabilidades en su software, lo cual podría permitir a los atacantes comprometer la seguridad del sistema y acceder a información sensible	
		RECOMENDACIÓN	
		Implementar un programa riguroso de actualización y parcheo para la aplicación de Python y todos sus módulos y bibliotecas. Asegurarse de que todos los componentes reciban las actualizaciones y parches de seguridad más recientes de manera oportuna, conforme a las mejores prácticas de la ISO 27001	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
16.2	Se identificó un riesgo considerable de que errores durante el mantenimiento o actualización del software afecten la funcionalidad de la aplicación de Python	Existe el riesgo de que errores durante el mantenimiento o actualización del software afecten la funcionalidad de la aplicación de Python, lo que podría resultar en interrupciones del servicio y disminución de la productividad.	
		RECOMENDACIÓN	
		Capacitar al personal técnico en las mejores prácticas de mantenimiento y actualización de software, incluyendo la identificación y corrección de errores comunes y la implementación segura de cambios. Esta capacitación debe alinearse con las directrices de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
17.1	Se identificó un riesgo significativo de exposición a vulnerabilidades en el sistema de registro de huellas, que podrían ser explotadas por atacantes	Existe el riesgo de que el sistema de registro de huellas sea vulnerable a ataques debido a vulnerabilidades en su software, lo cual podría permitir a los atacantes comprometer la seguridad del sistema y acceder a información biométrica sensible	
		RECOMENDACIÓN	
		Implementar cifrado fuerte para todos los datos biométricos almacenados y transmitidos por el sistema de registro de huellas. Asegurarse de que las claves de cifrado estén protegidas adecuadamente y que el acceso a ellas esté restringido.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
17.2	Se identificó un riesgo considerable de que errores durante el mantenimiento o actualización del software afecten la funcionalidad del sistema de registro de huellas.	Existe el riesgo de que errores durante el mantenimiento o actualización del software afecten la funcionalidad del sistema de registro de huellas, lo que podría resultar en interrupciones del servicio y disminuir la precisión y disponibilidad del registro biométrico.	
		RECOMENDACIÓN	
		Capacitar al personal técnico en las mejores prácticas de mantenimiento y actualización de software, incluyendo la identificación y corrección de errores comunes y la implementación segura de cambios. Esta capacitación debe alinearse con las directrices de la ISO 27001	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
18.1	Se identificó un riesgo significativo de exposición a vulnerabilidades en el sistema de puntaje de resultados, que podrían ser explotadas por atacantes	Existe el riesgo de que el sistema de puntaje de resultados sea vulnerable a ataques debido a vulnerabilidades en su software, lo cual podría permitir a los atacantes comprometer la seguridad del sistema y manipular los resultados.	
		RECOMENDACIÓN	
		Establecer mecanismos de autenticación y autorización robustos para el acceso al sistema de puntaje de resultados. Utilizar autenticación multifactor (MFA) y control de acceso basado en roles (RBAC) para limitar el acceso a información sensible y funciones críticas.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
18.2	Se identificó un riesgo considerable de que errores durante el mantenimiento o actualización del software afecten la precisión del sistema de puntaje.	Existe el riesgo de que errores durante el mantenimiento o actualización del software afecten la precisión del sistema de puntaje de resultados, lo que podría resultar en la generación de puntajes incorrectos y afectar la toma de decisiones basada en dichos resultados	
		RECOMENDACIÓN	
		Capacitar al personal técnico en las mejores prácticas de mantenimiento y actualización de software, incluyendo la identificación y corrección de errores comunes y la implementación segura de cambios. Esta capacitación debe alinearse con las directrices de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
20.1	Se identificó un riesgo significativo de exposición a vulnerabilidades en el software de Zoom, que podrían ser explotadas por atacantes	Existe el riesgo de que Zoom sea vulnerable a ataques debido a vulnerabilidades en su software, lo cual podría permitir a los atacantes comprometer la seguridad de las videoconferencias y acceder a información sensible	
		RECOMENDACIÓN	
		Asegurarse de que la aplicación de Zoom esté siempre actualizada con los últimos parches de seguridad y versiones más recientes. Implementar un sistema de actualización automática para minimizar la exposición a vulnerabilidades conocidas.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
20.2	Se identificó un riesgo considerable de que errores durante el mantenimiento o actualización del software afecten la seguridad y estabilidad de las videoconferencias en Zoom	Existe el riesgo de que errores durante el mantenimiento o actualización del software afecten la seguridad y estabilidad de las videoconferencias, lo que podría resultar en interrupciones del servicio y comprometer la confidencialidad de las comunicaciones.	
		RECOMENDACIÓN	
		Capacitar al personal técnico en las mejores prácticas de mantenimiento y actualización de software, incluyendo la identificación y corrección de errores comunes y la implementación segura de cambios. Esta capacitación debe alinearse con las directrices de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
21.1	Se identificó un riesgo significativo de daño o destrucción de los equipos por incendios.	Existe el riesgo de que los equipos sean dañados o destruidos por un incendio, lo cual podría resultar en la pérdida de datos críticos y afectar la continuidad operativa.	
		RECOMENDACIÓN	
		• Implementar sistemas de detección de incendios, como detectores de humo y calor, en todas las áreas donde se ubiquen equipos críticos. Instalar sistemas de extinción de incendios adecuados para entornos de TI, como rociadores automáticos y sistemas de gas inerte (por ejemplo, FM-200) que no dañen los equipos electrónicos. • Capacitar al personal en procedimientos de emergencia en caso de incendio, incluyendo el uso de extintores, la evacuación segura y la activación de sistemas de respuesta a incendios. Asegurar que todos los empleados conozcan las rutas de evacuación y los procedimientos de seguridad.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
21.2	Se identificó un riesgo considerable de daño a los equipos debido a inundaciones o fugas.	Existe el riesgo de que los equipos sufran daños por agua debido a inundaciones o fugas, lo cual podría resultar en la pérdida de funcionalidad y datos.	
		RECOMENDACIÓN	
		• Realizar inspecciones y mantenimiento regular de la infraestructura de plomería y sistemas de climatización para prevenir fugas y daños por agua. Asegurarse de que los sistemas de drenaje y bombas de agua funcionen correctamente. • Colocar los equipos en áreas que no sean propensas a inundaciones. Evitar ubicar equipos críticos en sótanos o áreas bajas que sean susceptibles a acumulación de agua. • Capacitar al personal en procedimientos de emergencia en caso de inundaciones o fugas, incluyendo la desconexión segura de equipos eléctricos y la protección de datos. Asegurar que todos los empleados conozcan los protocolos de emergencia.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
21.3	Se identificó un riesgo significativo de fallos en los equipos debido a problemas físicos.	Existe el riesgo de que los equipos fallen debido a desgaste o daños accidentales, afectando su operatividad.	
		RECOMENDACIÓN	
		• Implementar un programa de mantenimiento preventivo regular para todos los equipos críticos. Esto incluye la limpieza interna y externa de los equipos, la verificación de conexiones, la revisión de componentes y la actualización de firmware. • Desarrollar y aplicar políticas de uso para los equipos críticos, asegurando que solo el personal autorizado tenga acceso y pueda operar los equipos. Estas políticas deben incluir directrices claras sobre el manejo y el mantenimiento de los equipos.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
21.4	Se identificó un riesgo considerable de interrupciones en el funcionamiento por fallas eléctricas.	Existe el riesgo de que los equipos dejen de funcionar debido a cortes eléctricos, lo cual podría interrumpir las operaciones	
		RECOMENDACIÓN	
		• Implementar sistemas de alimentación ininterrumpida (UPS) para todos los equipos críticos. Los UPS proporcionarán energía temporal durante cortes eléctricos, permitiendo una transición suave a sistemas de respaldo o el apagado seguro de los equipos. • Capacitar al personal en procedimientos de emergencia para fallas eléctricas, incluyendo el uso de UPS y generadores, así como el apagado seguro de equipos. Asegurar que todos los empleados conozcan los prContratar seguros adecuados que cubran daños y pérdidas causadas por fallas eléctricas, asegurando que las operaciones puedan recuperarse rápidamente en caso de interrupciones prolongadas.otocolos de respuesta y recuperación.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
21.5	Se identificó un riesgo significativo de daño a los equipos por condiciones ambientales inadecuadas.	Existe el riesgo de que los equipos se dañen por altas temperaturas o humedad, afectando su rendimiento y durabilidad.	
		RECOMENDACIÓN	
		• Implementar sistemas de climatización adecuados en todas las áreas donde se ubiquen equipos críticos. Utilizar aire acondicionado y deshumidificadores para mantener la temperatura y la humedad dentro de los rangos óptimos para el funcionamiento de los equipos. • Instalar sensores para el monitoreo continuo de temperatura y humedad en las áreas donde se ubican los equipos. Utilizar sistemas de alerta que notifiquen al personal técnico en caso de que las condiciones ambientales se desvíen de los rangos seguros. • Realizar mantenimiento preventivo regular de todos los sistemas de climatización para asegurar su correcto funcionamiento. Esto incluye la limpieza de filtros, la revisión de componentes y la calibración de los sistemas.	

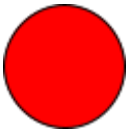
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
21.6	Se identificó un riesgo considerable de que errores en el mantenimiento afecten el funcionamiento de los equipos.	Existe el riesgo de que errores en el mantenimiento afecten el funcionamiento de los equipos, causando interrupciones y fallos.	
		RECOMENDACIÓN	
		• Capacitar al personal técnico en las mejores prácticas de mantenimiento de equipos. Asegurar que comprendan los procedimientos adecuados y los riesgos asociadoDesarrollar y ejecutar un plan de mantenimiento preventivo regular que incluya la inspección, limpieza y revisión de todos los equipos críticos. Esto ayuda a identificar y corregir problemas antes de que resulten en fallos.s con el mantenimiento incorrecto	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
21.7	Se identificó un riesgo significativo de extravío o pérdida de equipos.	Existe el riesgo de que los equipos se extravíen o se pierdan, lo cual podría resultar en la pérdida de datos y recursos.	
		RECOMENDACIÓN	
		• Establecer un sistema de inventario y registro detallado de todos los equipos. Asegurarse de que cada equipo esté etiquetado con un identificador único y que toda la información relevante (modelo, serie, ubicación, usuario asignado) se registre y actualice regularmente. • Desarrollar y aplicar políticas de seguridad física para el almacenamiento y uso de equipos. Esto incluye la restricción de acceso a áreas donde se guardan equipos críticos y la implementación de controles de entrada y salida. • Instalar cámaras de vigilancia y sistemas de monitoreo en áreas donde se almacenan equipos importantes	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
21.8	Se identificó un riesgo considerable de acceso no autorizado a los equipos.	Existe el riesgo de que personas no autorizadas accedan a los equipos, comprometiendo la seguridad de la información.	
		RECOMENDACIÓN	
		• Mantener un registro detallado de todas las personas que ingresan a áreas restringidas. Esto incluye el nombre, la hora de entrada y salida, y el propósito de la visita. Revisar regularmente estos registros para detectar cualquier actividad sospechosa. • Capacitar al personal sobre la importancia de la seguridad de los equipos y las políticas de acceso. Instruir a los empleados sobre cómo identificar y reportar actividades sospechosas.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
21.9	Se identificó un riesgo significativo de manipulación física no autorizada de los equipos.	Existe el riesgo de que los equipos sean manipulados físicamente sin autorización, lo cual podría causar daños o alteraciones en su funcionamiento.	
		RECOMENDACIÓN	
		Establecer controles de acceso físico estrictos en todas las áreas donde se encuentran los equipos críticos. Utilizar cerraduras y sistemas de autenticación biométrica para restringir el acceso únicamente al personal autorizado.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
21.10	Se identificó un riesgo considerable de robo de los equipos.	Existe el riesgo de que los equipos sean robados, lo cual podría resultar en la pérdida de datos sensibles y recursos materiales.	
		RECOMENDACIÓN	
		• Establecer controles de acceso físico estrictos para las áreas donde se encuentran los equipos críticos. Utilizar cerraduras y sistemas de autenticación biométrica para restringir el acceso a personal autorizado. • Instalar cámaras de vigilancia y sistemas de monitoreo en áreas donde se almacenan equipos importantes. Asegurarse de que las grabaciones se almacenen de manera segura y se revisen regularmente para detectar cualquier actividad sospechosa.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
21.11	Se identificó un riesgo significativo de daño intencional a los equipos por ataques físicos.	Existe el riesgo de que los equipos sean dañados intencionalmente, lo cual podría interrumpir las operaciones y causar pérdidas financieras.	
		RECOMENDACIÓN	
		Establecer controles de acceso físico estrictos para las áreas donde se encuentran los equipos críticos. Utilizar cerraduras y sistemas de autenticación biométrica para restringir el acceso a personal autorizado.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
22.1	Se identificó un riesgo significativo de daño o destrucción de los equipos por incendios.	Existe el riesgo de que los equipos sean dañados o destruidos por un incendio, lo cual podría resultar en la pérdida de datos críticos y afectar la continuidad operativa.	
		RECOMENDACIÓN	
		• Implementar sistemas de detección de incendios, como detectores de humo y calor, en todas las áreas donde se ubiquen equipos críticos. Instalar sistemas de extinción de incendios adecuados para entornos de TI, como rociadores automáticos y sistemas de gas inerte (por ejemplo, FM-200) que no dañen los equipos electrónicos. • Capacitar al personal en procedimientos de emergencia en caso de incendio, incluyendo el uso de extintores, la evacuación segura y la activación de sistemas de respuesta a incendios. Asegurar que todos los empleados conozcan las rutas de evacuación y los procedimientos de seguridad.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
22.2	Se identificó un riesgo considerable de daño a los equipos debido a inundaciones o fugas.	Existe el riesgo de que los equipos sufran daños por agua debido a inundaciones o fugas, lo cual podría resultar en la pérdida de funcionalidad y datos.	
		RECOMENDACIÓN	
		• Capacitar al personal en procedimientos de emergencia en caso de inundaciones o fugas, incluyendo la desconexión segura de equipos eléctricos y la protección de datos. Asegurar que todos los empleados conozcan los protocolos de emergencia. • Realizar inspecciones y mantenimiento regular de la infraestructura de plomería y sistemas de climatización para prevenir fugas y daños por agua. Asegurarse de que los sistemas de drenaje y bombas de agua funcionen correctamente.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
22.3	Se identificó un riesgo significativo de fallos en los equipos debido a problemas físicos.	Existe el riesgo de que los equipos fallen debido a desgaste o daños accidentales, afectando su operatividad	
		RECOMENDACIÓN	
		• Implementar un programa de mantenimiento preventivo regular para todos los equipos críticos. Esto incluye la limpieza interna y externa de los equipos, la verificación de conexiones, la revisión de componentes y la actualización de firmware. • Realizar inspecciones periódicas de todos los equipos para identificar signos de desgaste o daño. Estas inspecciones deben ser detalladas y documentadas para asegurar que se tomen las acciones correctivas necesarias.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
22.4	Se identificó un riesgo considerable de interrupciones en el funcionamiento por fallas eléctricas	Existe el riesgo de que los equipos dejen de funcionar debido a cortes eléctricos, lo cual podría interrumpir las operaciones.	
		RECOMENDACIÓN	
		• Implementar sistemas de alimentación ininterrumpida (UPS) para todos los equipos críticos. Los UPS proporcionarán energía temporal durante cortes eléctricos, permitiendo una transición suave a sistemas de respaldo o el apagado seguro de los equipos. • Realizar mantenimiento preventivo regular de todos los sistemas eléctricos, incluyendo cables, interruptores y paneles de distribución. Asegurarse de que todos los componentes eléctricos cumplan con los estándares de seguridad y funcionamiento.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
22.5	Se identificó un riesgo significativo de daño a los equipos por condiciones ambientales inadecuadas.	Existe el riesgo de que los equipos se dañen por altas temperaturas o humedad, afectando su rendimiento y durabilidad	
		RECOMENDACIÓN	
		• Implementar sistemas de climatización adecuados en todas las áreas donde se ubiquen equipos críticos. Utilizar aire acondicionado y deshumidificadores para mantener la temperatura y la humedad dentro de los rangos óptimos para el funcionamiento de los equipos. • Instalar sensores para el monitoreo continuo de temperatura y humedad en las áreas donde se ubican los equipos. Utilizar sistemas de alerta que notifiquen al personal técnico en caso de que las condiciones ambientales se desvíen de los rangos seguros.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
22.6	Se identificó un riesgo considerable de que errores en el mantenimiento afecten el funcionamiento de los equipos.	Existe el riesgo de que errores en el mantenimiento afecten el funcionamiento de los equipos, causando interrupciones y fallos.	
		RECOMENDACIÓN	
		Desarrollar y ejecutar un plan de mantenimiento preventivo regular que incluya la inspección, limpieza y revisión de todos los equipos críticos. Esto ayuda a identificar y corregir problemas antes de que resulten en fallos.	

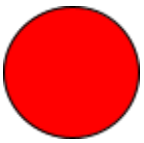
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
22.7	Se identificó un riesgo significativo de extravío o pérdida de equipos.	Existe el riesgo de que los equipos se extravíen o se pierdan, lo cual podría resultar en la pérdida de datos y recursos.	
		RECOMENDACIÓN	
		• Establecer un sistema de inventario y registro detallado de todos los equipos. Asegurarse de que cada equipo esté etiquetado con un identificador único y que toda la información relevante (modelo, serie, ubicación, usuario asignado) se registre y actualice regularmente. • Desarrollar y aplicar políticas de seguridad física para el almacenamiento y uso de equipos. Esto incluye la restricción de acceso a áreas donde se guardan equipos críticos y la implementación de controles de entrada y salida.	

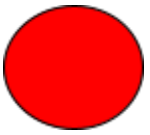
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
22.8	Se identificó un riesgo considerable de acceso no autorizado a los equipos.	Existe el riesgo de que personas no autorizadas accedan a los equipos, comprometiendo la seguridad de la información.	
		RECOMENDACIÓN	
		• Establecer controles de acceso físico estrictos en todas las áreas donde se encuentran los equipos críticos. Utilizar cerraduras y sistemas de autenticación biométrica para restringir el acceso a personal autorizado.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
22.9	Se identificó un riesgo significativo de manipulación física no autorizada de los equipos.	Existe el riesgo de que los equipos sean manipulados físicamente sin autorización, lo cual podría causar daños o alteraciones en su funcionamiento	
		RECOMENDACIÓN	
		• Establecer controles de acceso físico estrictos en todas las áreas donde se encuentran los equipos críticos. Utilizar cerraduras y sistemas de autenticación biométrica para restringir el acceso únicamente al personal autorizado. • Desarrollar y documentar políticas de seguridad física claras y rigurosas. Estas políticas deben incluir directrices sobre el acceso a áreas restringidas, el manejo de equipos y la respuesta a incidentes de seguridad.	

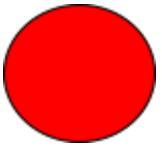
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
22.10	Se identificó un riesgo considerable de robo de los equipos.	Existe el riesgo de que los equipos sean robados, lo cual podría resultar en la pérdida de datos sensibles y recursos materiales.	
		RECOMENDACIÓN	
		• Instalar cámaras de vigilancia y sistemas de monitoreo en áreas donde se almacenan equipos importantes. Asegurarse de que las grabaciones se almacenen de manera segura y se revisen regularmente para detectar cualquier actividad sospechosa. • Establecer controles de acceso físico estrictos para las áreas donde se encuentran los equipos críticos. Utilizar cerraduras, tarjetas de acceso y sistemas de autenticación biométrica para restringir el acceso al personal autorizado.	

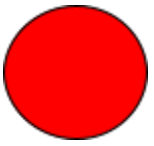
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
22.11	Se identificó un riesgo significativo de daño intencional a los equipos por ataques físicos.	Existe el riesgo de que los equipos sean dañados intencionalmente, lo cual podría interrumpir las operaciones y causar pérdidas financieras.	
		RECOMENDACIÓN	
		• Capacitar al personal en la importancia de la seguridad de los equipos y en los procedimientos para prevenir daños intencionales. Instruir sobre cómo identificar y reportar actividades sospechosas o inusuales. • Mantener un registro detallado de todas las personas que ingresan a áreas restringidas. Esto incluye el nombre, la hora de entrada y salida, y el propósito de la visita. Revisar regularmente estos registros para detectar cualquier actividad sospechosa.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificó un riesgo de desastres naturales para las instalaciones de la Dirección de Admisión. Fenómenos como lluvias frecuentes,tormentas u otros desastres naturales pueden causar daños significativos a la infraestructura y equipos, comprometiendo la operación continua y la integridad de los datos.	• Daños materiales significativos. • Pérdida de datos.	
		RECOMENDACIÓN	
		Implementar un plan de contingencia y refuerzo estructural conforme a las normativas de construcción y seguridad aplicables para mitigar el riesgo de desastres naturales, alineado con las directrices de ISO 22301:2012 (Sistemas de Gestión de Continuidad del Negocio), ISO 31000:2018 (Gestión del Riesgo), ISO 45001:2018 (Sistemas de Gestión de Seguridad y Salud en el Trabajo), y los códigos de construcción y normativas locales, asegurando así que las medidas sean efectivas en la protección contra incidentes disruptivos y desastres naturales.	

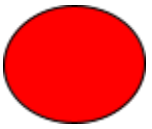
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificó un riesgo de pérdida de equipos en las instalaciones de la Dirección de Admisión. La pérdida de equipos, ya sea accidental o intencional, puede afectar la operatividad y disponibilidad de la información crítica, interrumpiendo los procesos administrativos y de admisión.	• Interrupciones en el servicio. • Pérdida de datos.	
		RECOMENDACIÓN	
		Implementar inventarios regulares y medidas de seguridad física para proteger los equipos críticos y mitigar el riesgo de pérdida de equipos, conforme a las directrices de la ISO/IEC 27001:2013, alineado con los controles A.8.1.1 (Inventario de activos), A.11.1.1 (Seguridad física perimetral), A.11.2.1 (Equipos en áreas seguras) y A.11.2.4 (Protección contra amenazas externas y ambientales), asegurando así la protección y disponibilidad de los equipos críticos y la continuidad de los procesos administrativos y de admisión.	

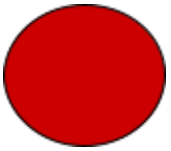
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificó un riesgo de abuso de privilegios de acceso en las instalaciones de la Dirección de Admisión. Personal con acceso privilegiado puede utilizar sus derechos para acceder indebidamente a información crítica y posiblemente manipular datos.	• Acceso indebido a información crítica. • Posible manipulación de datos.	
		RECOMENDACIÓN	
		Implementar controles de acceso estrictos, auditorías regulares y un sistema de control para verificar el historial de acceso para mitigar el riesgo de abuso de privilegios, conforme a las directrices de la ISO/IEC 27001:2013, alineado con los controles A.9.2.3 (Gestión de acceso privilegiado), A.9.4.1 (Uso de privilegios del sistema), A.12.4.3 (Registro de acceso privilegiado) y A.12.7.1 (Revisión de eventos de auditoría), asegurando así que el acceso a información crítica esté adecuadamente controlado, monitoreado y revisado para prevenir el acceso indebido y la manipulación de datos.	

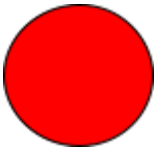
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificó un riesgo de robo de equipos en las instalaciones de la Dirección de Admisión. El robo de equipos puede resultar en la pérdida de datos y de recursos tecnológicos críticos para la operatividad del área.	• Pérdida de datos. • Pérdida de equipos críticos.	
		RECOMENDACIÓN	
		Implementar sistemas de seguridad física, como cámaras de vigilancia, controles de acceso biométricos y guardias de seguridad, junto con medidas de control de acceso, para proteger los equipos críticos y mitigar el riesgo de robo de equipos, conforme a las directrices de la ISO/IEC 27001:2013, alineado con los controles A.11.1.1 (Seguridad física perimetral), A.11.1.2 (Controles de entrada física), A.11.2.1 (Equipos en áreas seguras) y A.11.2.7 (Seguridad del equipo fuera de las instalaciones), asegurando así la protección de los recursos tecnológicos y la continuidad operativa del área.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificó un riesgo de ataques destructivos en las instalaciones de la Dirección de Admisión. Estos ataques pueden causar daños materiales significativos y comprometer la seguridad de la información almacenada y procesada en estas instalaciones.	• Daños materiales. • Compromiso de la seguridad de la información.	
		RECOMENDACIÓN	
		Implementar medidas de protección física, como puertas reforzadas, ventanas blindadas y sistemas de alarma, junto con el monitoreo continuo mediante cámaras de vigilancia y sensores de movimiento, para mitigar el riesgo de ataques destructivos en las instalaciones de la Dirección de Admisión. Esto debe realizarse conforme a las directrices de la ISO/IEC 27001:2013, alineado con los controles A.11.1.1 (Seguridad física perimetral), A.11.1.2 (Controles de entrada física), A.11.1.4 (Protección contra amenazas externas y ambientales) y A.12.4.1 (Registro de	

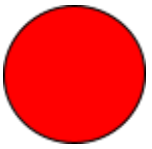
		eventos), asegurando así la integridad de las instalaciones y la seguridad de la información almacenada y procesada.

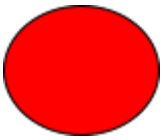
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificó un riesgo de ocupación en las instalaciones de la Dirección de Admisión .La toma de control por personas no autorizadas puede resultar en el acceso indebido a información crítica y comprometer la seguridad de las operaciones.	• La toma de control de las instalaciones por personas no autorizadas puede resultar en el acceso indebido a información crítica y comprometer la seguridad de las operaciones. Esto podría llevar a la divulgación de datos sensibles, manipulación de documentos oficiales y afectación de la integridad del proceso de admisión.	
		RECOMENDACIÓN	
		Implementar protocolos de seguridad y respuesta a incidentes conforme a las directrices de la ISO/IEC 27001:2013. Esto incluye establecer procedimientos claros para la identificación y reporte de incidentes de seguridad, designar un equipo de respuesta a incidentes, y realizar simulaciones periódicas de incidentes para asegurar la preparación. También se deben implementar medidas de seguridad física, como vigilancia y controles de acceso, para prevenir la ocupación no autorizada de las instalaciones.	

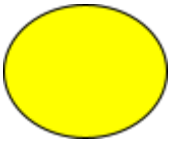
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificó un riesgo de incendio en los UPS y equipos de cómputo en las instalaciones. Este riesgo puede resultar en la destrucción de equipos y pérdida de datos críticos, comprometiendo la continuidad de las operaciones y la seguridad de la información.	• Pérdida de equipos y datos. • Afectación de la operatividad.	
		RECOMENDACIÓN	
		Implementar sistemas de detección y extinción de incendios, y realizar simulacros de evacuación periódicos conforme a las directrices de la ISO 27001 para mitigar el riesgo de incendio.	

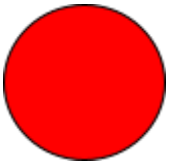
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificaron errores de mantenimiento y actualización en los equipos de computo en las instalaciones. Estos errores pueden provocar fallos en la integridad y disponibilidad de los datos, comprometiendo la operatividad y la seguridad de la información.	• Fallos en la integridad de los datos. • Fallos en la disponibilidad de los datos. • Interrupción de operaciones.	
		RECOMENDACIÓN	
		Implementar procedimientos rigurosos de mantenimiento y actualización conforme a las directrices de la ISO 27001 y la ISO 27002 para mitigar los errores de mantenimiento y actualización.	

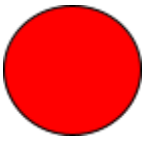
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificó un riesgo de uso no previsto de los UPS y equipos de cómputo en las instalaciones. El uso indebido o no autorizado de estos equipos puede llevar a comprometer la seguridad de la información, causar desgaste prematuro del equipo, interrupciones del servicio, sobrecarga del sistema, conflictos de recursos, consumo ineficiente de energía,, incompatibilidades del sistema, exposición a vulnerabilidades, y costos adicionales de mantenimiento.	• La alteración de procesos críticos puede afectar la continuidad operativa y la eficiencia de la organización. • El uso excesivo o inapropiado puede sobrecargar los sistemas, disminuyendo su rendimiento. • El uso no previsto puede introducir nuevas vulnerabilidades de seguridad, aumentando el riesgo de ciberataques.	
		RECOMENDACIÓN	
		Establecer políticas claras de uso y acceso a los equipos auxiliares, y monitorear las actividades conforme a las directrices de la ISO 27001. Implementar procedimientos de capacitación para el personal y realizar auditorías regulares para asegurar el cumplimiento de las políticas de uso y acceso.	

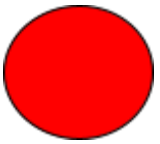
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificó un riesgo de manipulación indebida del hardware en los equipos de cómputo en las instalaciones. La manipulación no autorizada puede causar fallos en la seguridad del sistema, pérdida de datos, interrupciones operativas y costos adicionales de reparación y mantenimiento.	• La manipulación no autorizada del hardware puede comprometer la integridad de los datos, afectar la operatividad del sistema, introducir vulnerabilidades, provocar la pérdida de datos y causar interrupciones operativas, además de generar costos adicionales de reparación y mantenimiento.	
		RECOMENDACIÓN	
		Implementar controles de acceso físico y monitoreo continuo de los equipos conforme a las directrices de la ISO 27001 para mitigar el riesgo de manipulación del hardware. Establecer políticas de seguridad estrictas, realizar auditorías regulares y capacitar al personal sobre la importancia de la seguridad del hardware.	

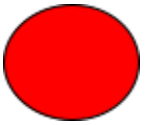
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificaron posibles ataques de denegación de servicio (DoS) en el servidor FTP, lo que provoca interrupciones en el servicio y afecta la disponibilidad de los recursos durante el proceso de admisión.	• Interrupciones en el servicio, afectando la disponibilidad de los recursos y la continuidad del proceso de admisión.	
		RECOMENDACIÓN	
		Se recomienda elaborar e implementar un plan de prevención contra ataques DoS, así como la adopción de medidas de seguridad adicionales para mitigar este riesgo conforme a las directrices de la ISO 27001.	

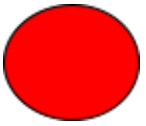
Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se detectó que se pueden enviar correos maliciosos a través de las redes de comunicaciones, con la finalidad de obtener información confidencial utilizando técnicas de ingeniería social.	• Los ataques de phishing pueden comprometer la seguridad de la información y llevar al robo de datos confidenciales, afectando la integridad y confidencialidad del proceso de admisión.	
		RECOMENDACIÓN	
		Implementar protocolos de autenticación, como DKIM (DomainKeys Identified Mail), para verificar la autenticidad de los correos electrónicos entrantes y reducir el riesgo de phishing, conforme a las directrices de la ISO 27002.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se identificó un riesgo de manipulación no autorizada de información en el gestor de bases de datos, comprometiendo la integridad y exactitud de los datos almacenados.	• La manipulación no autorizada de datos en la base de datos puede resultar en la alteración, corrupción o pérdida de datos críticos, afectando la integridad y disponibilidad de la información.	
		RECOMENDACIÓN	
		Realizar copias de seguridad periódicas de la base de datos y establecer un plan de recuperación ante desastres para asegurar la restauración de datos, conforme a las directrices de la ISO 27001.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Se detectó además que el director de la oficina de OTI tiene acceso privilegiado a la información de la base de datos.	La alteración no autorizada de la información puede comprometer la integridad y confidencialidad de los datos críticos almacenados.	
		RECOMENDACIÓN	
		Implementar controles y mecanismos que limiten el acceso y gestión de la base de datos a personal autorizado, evitando que una sola persona tenga control completo sobre la información crítica. Registrar y monitorear cualquier actividad sospechosa o inapropiada, y realizar auditorías regulares para asegurar la integridad y seguridad de los datos	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Compromiso de la confidencialidad, integridad y disponibilidad de la información en la universidad.	Fugas de información.	
		RECOMENDACIÓN	
		Establecer políticas claras de confidencialidad que especifique qué información se considera confidencial y los métodos de protección. Implementar un sistema de autenticación y autorización robusto, así como la realización de auditorías regulares para asegurar la integridad y seguridad de los datos.	

Proceso:		Área: Oficina de admisión	Nivel de riesgo
Nº	Hallazgo	Riesgo Potencial	
0	Divulgación de información confidencial, modificación o alteración de datos, y uso indebido de recursos por parte de los practicantes que laboran en la OTI.	• Compromiso de la confidencialidad, integridad y disponibilidad de la información.	
		RECOMENDACIÓN	
		Establecer políticas claras de confidencialidad que especifiquen qué información se considera confidencial y los métodos de protección, conforme a las directrices de la ISO/IEC 27001:2013. Implementar medidas de control de acceso basadas en roles para limitar el acceso a la información confidencial (Control A.9.1.2). Definir políticas de uso aceptable de los recursos de la OTI, incluyendo equipos informáticos y sistemas, y proporcionar capacitación regular a los practicantes sobre estas políticas. Realizar auditorías periódicas para asegurar el cumplimiento de las políticas y detectar cualquier uso indebido de recursos (Control A.12.7.1). Además, utilizar herramientas de monitoreo y registro de actividad para supervisar el acceso y uso de los datos y sistemas (Control A.12.4.1).	

<table>
<tr><td colspan="2">Proceso:</td><td>Área: Oficina de admisión</td><td>Nivel de riesgo</td></tr>
<tr><td>Nº</td><td>Hallazgo</td><td>Riesgo Potencial</td><td></td></tr>
<tr><td rowspan="3">0</td><td rowspan="3">Se identificó un riesgo de caída del sistema debido a la sobrecarga de recursos en la red local. Esta situación ha provocado que durante el registro de postulantes, el sistema se paralice y cree un cuello de botella, afectando la fluidez y eficiencia del proceso.</td><td>● La caída del sistema puede interrumpir el registro de postulantes, causando retrasos significativos.
● La sobrecarga de recursos puede comprometer la operatividad y disponibilidad de la red local.</td><td>  </td></tr>
<tr><td colspan="2">RECOMENDACIÓN</td></tr>
<tr><td colspan="2">Implementar medidas de monitoreo y gestión de recursos de la red para identificar y prevenir sobrecargas, conforme a las directrices de la ISO/IEC 27001:2013. Esto incluye el uso de herramientas de monitoreo en tiempo real como Nagios y Zabbix, la implementación de balanceadores de carga para distribuir el tráfico de manera equitativa, y la optimización de la configuración de los routers y switches. Además, aumentar la capacidad de la infraestructura de red mediante la actualización de hardware y la ampliación del ancho de banda. Realizar pruebas de estrés periódicas utilizando herramientas como Apache JMeter y Wireshark para asegurar que la red puede manejar el volumen esperado de tráfico sin problemas. Esto se alinea con los controles A.12.1.3 (Capacidad de los sistemas de información), A.12.4.1 (Registro de eventos), A.12.6.1 (Gestión de vulnerabilidades técnicas) y A.13.1.1 (Gestión de la seguridad de la red) de la ISO/IEC 27001:2013.</td></tr>
</table>