Certificación de sistemas de gestión
Informe de resumen de auditoría

Organización:	**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD**				
Dirección:	Calle 14 Sur #14 - 23, Bogotá D.C., Colombia				
Estándar(s):	***ISO/IEC 27001:2022***		Organismo(s) de Acreditación: UNACC		
Representante:	Rafael Ramírez (Gerente de Plataformas e Infraestructura Tecnológica)				
Sitios auditados:	Calle 14 Sur #14 - 23, Bogotá D.C., Colombia		Fecha(s) de la(s) auditoría(s):	1, 5 y 6 de Noviembre de 2024 (2.5 días)	
Código EAC:	33, 37	Código NACE:	72.2, 80.3	Código del área técnica:	IS 22 IS 25
N.ó ón eficaz del Personal:	11		No. de Turnos:	1	
Auditor principal:	Alexandra Bibiana Cala Moreno. Ext.alexandra.cala@sgs.com, Cel 3144682901		Miembro o miembros adicionales del equipo:	N.A.	
Asistentes y funciones adicionales:	N.A				
Este informe es confidencial, y la distribución se limita al equipo de la auditoría, los asistentes a la auditoría, el representante del cliente, la oficina de SGS y puede estar sujeto a un organismo de acreditación, a los propietarios del programa de certificación o a cualquier otro organismo regulador en línea con nuestra Declaración de privacidad en línea a la que se puede acceder. Aquí					

1. Objetivos de la auditoría

Los objetivos de esta auditoría eran:
Para determinar la conformidad del sistema de gestión, o de partes del mismo con criterios de auditoría y sus:

- *capacidad para garantizar el cumplimiento de los requisitos legales, reglamentarios y contractuales aplicables,*
- *para asegurar que el cliente pueda esperar razonablemente lograr los objetivos especificados, y*
- *capacidad de identificar, según sea aplicable, las áreas que puedan mejorarse.*

2. Ámbito de la certificación

Realizar el Servicio de Auditoría Interna al Sistema de Seguridad de la Información de la compañía UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD, acorde con los requisitos de la norma ISO 27001:2022, a su sede principal ubicada en la ciudad de Bogotá D.C.

Realizar el Servicio de Auditoría Interna al Sistema de Seguridad de la Información de la UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD, acorde con los requisitos de la norma ISO 27001:2022, a su sede principal ubicada en la ciudad de Bogotá D.C.

¿Se ha modificado este ámbito como resultado de esta auditoría? ☐ Sí ☒ No

El código o códigos ea indicados en este encabezado del informe ha(n) sido evaluado y se ha encontrado que es el correcto para describir mejor las actividades realizadas en esta organización, en línea con el ámbito de certificación. ☒ Sí

Se trata de una auditoría de varios sitios y un apéndice que enumera todos los sitios relevantes y/o ubicaciones remotas se ha establecido (adjunta) y se ha acordado con el cliente. ☐ Sí ☒ No

Para auditorías integradas, confirme el nivel actual de integración de IMS del cliente: ☒ N/A ☐ Básica ☐ Alto

3. Conclusiones y conclusiones actuales de la auditoría

El equipo de la auditoría realizó una auditoría basada en procesos, centrada en aspectos/riesgos/objetivos significativos exigidos por los estándares. Se utilizó un proceso de toma de muestras a partir de la información disponible en el momento de la auditoría. Los métodos de auditoría utilizados fueron entrevistas, observación de actividades y revisión de documentación y registros.
La estructura de la auditoría se encontraba en conformidad con el plan de auditoría incluido como anexo a este informe resumido.
El equipo de la auditoría termina que la organización ☒ tiene ☐ no ha establecido y mantenido su sistema de gestión en línea con los requisitos de la norma y demostrado la capacidad del sistema para lograr de forma sistemática los requisitos acordados para los productos o servicios en el ámbito, así como la normativa y los objetivos de la organización.

Número de no conformidades identificadas:	0	Destacado		Menor	

Por ello, el equipo de auditorías recomienda que, en función de los resultados de esta auditoría y del estado demostrado de desarrollo y madurez del sistema, la certificación del sistema de gestión sea:

N.A. Dado que es Auditoría Interna.

☐ Concedido/ ☐ Continuó/ ☐ Retenido/ ☐ Se suspenden hasta que se completen las acciones correctivas satisfactorias.

4. Resultados de la auditoría anterior (N.A. por ser Auditoría Interna)

Los resultados de la última auditoría de este sistema han sido revisados, de manera concreta para asegurar la corrección adecuada y se han implementado medidas correctivas para hacer frente a cualquier no conformidad identificada. Esta revisión ha finalizado que:

☐ Cualquier no conformidad identificada durante las auditorías anteriores ha sido corregida y la acción correctiva sigue siendo eficaz. (Consulte la sección 6 para obtener más información)

☐ El sistema de gestión no ha abordado adecuadamente la no conformidad identificada durante las actividades de auditoría anteriores y el problema específico se ha definido de nuevo en la sección de no conformidad de este informe.

5. Hallazgos de la auditoría

El equipo de la auditoría realizó una auditoría basada en procesos, centrada en aspectos/riesgos/objetivos significativos. Los métodos de auditoría utilizados fueron entrevistas, observación de actividades y revisión de documentación y registros.

La documentación del sistema de gestión demuestra la conformidad con los requisitos de la norma de auditoría y proporciona la estructura suficiente para apoyar la implementación y el mantenimiento del sistema de gestión.	☐ Sí	☒ No
La organización ha demostrado una implementación y mantenimiento/ mejora eficaces de su sistema de gestión, y es capaz de lograr sus objetivos político., así como los resultados esperados de los respectivos sistemas de gestión.	☐ Sí	☒ No
'La organización ha demostrado una implementación y un seguimiento efectivos de la capacidad de su sistema de gestión en relación con el cumplimiento de los requisitos legales, reglamentarios y contractuales aplicables.	☐ Sí	☒ No
La organización ha demostrado el establecimiento y el seguimiento de los objetivos y objetivos de rendimiento clave adecuados, así como ha supervisado el progreso hacia su logro.	☐ Sí	☒ No
El programa de auditoría interna se ha implementado plenamente y demuestra la eficacia como herramienta para mantener y mejorar el sistema de gestión.	☒ Sí	☐ No
El proceso de revisión de la gestión demuestra la capacidad para asegurar la idoneidad, adecuación y eficacia continuadas del sistema de gestión.	☐ Sí	☒ No
A lo largo del proceso de auditoría, el sistema de gestión mostró una conformidad general con los requisitos de la norma de auditoría.	☐ Sí	☒ No
Las reclamaciones de certificación son exactas y de acuerdo con la orientación de SGS, y la organización controla eficazmente el uso de documentos y marcas de certificación.	☒N/A ☐ Sí	☐ No

6. seguimiento de auditorías significativas seguidas

Los procesos, actividades y funciones específicas revisados se detallan en la Matriz de planificación de la auditoría y en el plan de auditoría. En la realización de la auditoría, se desarrollaron varios seguimientos de auditorías y vínculos, incluyendo el siguiente seguimiento de auditoría principal, seguido a través de:

- En relación con los resultados de auditorías anteriores:

N.A.

- En relación con esta auditoría; incluyendo cualquier cambio significativo (por ejemplo: al personal clave, las actividades de los clientes, el sistema de gestión, el nivel de integración, etc.):

Contexto de la Organización.
Se tienen identificados los siguientes procesos:

1. Gestión de la información y del conocimiento organizacional
2. Planificación Institucional

3. Mejoramiento de la Gestión Organizacional
4. Gestión de Servicios de Infraestructura Tecnológica
5. Gestión y Desarrollo de la Plataforma Humana
6. Gestión de Recursos Físicos Administrativos y Financieros
7. Gestión Integral de la Infraestructura Física
8. Gestión de la Seguridad de la Información, Ciberseguridad y Continuidad Operacional de la Organizacional
9. Evaluación de Aseguramiento de la Gestión Organizacional.

No se tienen identificados los numerales y controles aplicables a cada proceso.
No se tiene contexto de la organización documentado

Partes Interesadas.
Se tiene en la matriz de Stakeholders (Partes Interesadas), está en proceso de documentación.

Clasificación y Etiquetado.
Se tiene pública para la información de archivo, para la información en gestión no se tiene etiquetado y clasificación a la fecha.

Política.
Se tiene documentada dentro del Manual del SIG M.1 Versión 22 del 28 de agosto de 2023. Se encuentra pública dentro de la página WEB.

Riesgos:
Se tiene metodología basada en Magerit.
No se tiene identificado el dueño del riesgo
Se está en proceso de levantamiento la matriz. Garantizar que se genere la aceptación del riesgo residual y del Plan de Tratamiento de los riesgos.

Indicadores:
Se tienen identificados:
- Atención a los incidentes de seguridad de la información reportados
- Sanitización de las vulnerabilidades identificadas en los activos críticos de la información.

Revisar y reportar mas indicadores.

Objetivo:
Proteger y preservar la información física, electrónica y digital de la institución, almacenada en los diferentes activos de la información, salvaguardando su confidencialidad, integridad y disponibilidad, atendiendo los lineamientos de la política de Gestión Documental, promoviendo una cultura de seguridad y adaptación a los cambios relacionados con la continuidad del negocio.

No se tienen planes para alcanzar el objetivo

No se tiene declaración de aplicabilidad

Controles:
A.5.1. Se tiene resolución 007298 del 10 de mayo de 2023.Marco de referencia del SGSI, se tienen las siguientes políticas: Dispositivos móviles, Control de Acceso Lógico, Uso de controles Criptográficos, Transferencia e Intercambio de información, Desarrollo Seguro. Escritorio y Pantalla Limpios, Gestión del Cambio. Respaldo y Continuidad de la Operación, Gestión Administrativa y Conservación Documental, Incidentes de Seguridad de la Información, Uso Aceptable de los Activos, Eliminación Segura de la Información, Proveedores, Gestión en la Nube.

Falta política de Continuidad y de Clasificación,

A.5.3 Se tiene evidencia de la separación de funciones por medio de la asignación de permisos

A.5.4 Se evidencia compromiso de la alta Dirección frente al SGSI.

A.5.5 y A.5.6. Se tiene plan de comunicaciones. Relacionar todas las Entidad como contacto con autoridades. No se tiene identificados los grupos de interés

A.5.7 No se tiene analisis sobre la información entregada por el Csirt que permita generar inteligencia de amenazas.

A.5.8 No se tienen identificados los riesgos de seguridad de la información en la gestión de proyectos, tal es el caso del proyecto del DRP

A.5.9 y A.5.10 Se tiene inventario de activos, se tiene política uso aceptable de los activos

A.5.11 Se tiene evidencia de la devolución de activos

A.5.12 y A.5.13 Se tiene pública para la información de archivo, para la información en gestión no se tiene etiquetado y clasificación a la fecha.

A.5.14 Se tiene control sobre la transferencia de información.

A.5.15 No se tiene documentada la matriz de acceso

A.5.16, A.5.17, A.5.18 Se tiene para Google y para Microsoft. No todo tiene doble factor de autenticación

A.5.19, A.5.20, A.5.21, A.5.22. Se controla desde ISO 9001 pero no se tienen identificados riesgos de proveedores

A.5.23 Se tiene servicios en la nube se tiene procedimiento.

A.5.24, A.5.25, A.5.26, A.5.27, A.5.28 Se tienen identificados incidentes; sin embargo, no se tiene toda la gestión sobre los mismos

A.5.29 y A.5.30 No se tiene plan de continuidad y el DRP está en proceso de construcción

A.5.37 Se tiene Instructivo para Respaldo de Información, Procedimiento de Backups

A.6.1 Se tiene revisión de antecedentes antes de la vinculación laboral. Se tiene para docentes y contratistas de manera anual
A.6.2 Se tienen definidas los roles y responsabilidades frente al SGSI, dentro del contrato.
A.6.3. Se tiene plan de capacitación anual, se hace a principio de año consolidando las necesidades de todos las áreas en SGSI se tiene: Seguridad de la información, Gestión de Usuarios, también se tiene dentro del plan las inducciones y reinducciones.
A.6.4 Proceso Disciplinario
A.6.5. No se tiene tiempo de permanencia para manejo de temas de seguridad de la información que después del retiro. Se devolución de activos.
A.6.6. Se tienen acuerdos de confidencialidad firmada
A.6.7. Se tiene establecido por resolución para manejo de trabajo Híbrido.
A.6.8. Se tiene dentro de la inducción.

A.7.1, A.7.2, A.7.3, A.7.4. Se tiene cámaras se tiene control 7 x 24, Se manejan dos garitas uno para vehículos oriental y occidental. Se tienen talanqueras que impiden el ingreso de personal externo a la organización, se tiene biométrico la Gerencia de Talento Humano tiene control sobre la base de datos. Para los externos. No se tiene divulgación de la política de datos personales al recopilar información para el ingreso de personal.

No se tiene evidencia de la divulgación de la política de seguridad de la información

A.7.5 Se tiene extintores y se tienen rutas de evacuación correspondientes, se hace simulacro de evacuación.

A.7.7 Se tienen accesos directos en los computadores, se tiene firma del Gerente de Infra, Ingreso a Pinterest,

A.7.8, A.7.9. El control de los equipos en la organización se controla por medio de las cámaras y seguridad física, para la salida de equipos se tiene que diligenciar un formato Autorización Salida de Bienes y el ingreso se vuelve a validar.

A.7.10. No se manejan, Validar la No Aplicabilidad

A.7.11 Mantenimiento UPS Se realiza una vez al año no se tiene evidencia de dicha actividad y Planta Eléctrica. Se hace por parte de un tercero en Junio de 2024

A.7.12 Se tiene control por medio de etiquetado lógico

A.7.13 Se tiene por contrato del Proveedor de Leasing, se realiza 1 vez al año, lo realiza directamente el proveedor. Se tiene cronograma correspondiente

A.7.14 Todos son por Leasing y se hace devolución cuando termina el contrato, no queda evidencia del borrado.

A.8.1 Las personas que traen sus equipos personales se conectan a la red de invitados.

A.8.2 No se tienen documentados los permisos que tiene cada uno de los funcionarios

A.8.3 Se da por medio de los permisos asignados, el responsable del servicio es el encargado de dar los permisos correspondientes.

A.8.4. Se tiene documentado en las historias de usuario, También se tiene en la plataforma GitLab, tiene acceso los desarrolladores. Se tiene Manual de estilos Factoría de Software Plataforma AUREA, del 6 de noviembre de 2020.

A.8.5 Se tiene control por usuario y contraseña, para el otro año se está empezando a trabajar doble factor de autenticación, las aplicaciones de Google si se tienen controladas con doble factor de autenticación.
Se tiene proyecto denominado Sistema Único de Autenticación. En el Diseño se tiene estipulados los temas de seguridad no se tienen identificados. Los riesgos tampoco se tienen identificados.

A.8.6 Capacidad: Se tiene Herramienta HPE InfoSight, Se tiene capacidad utilizada del 11%. Cada 5 años se hace renovación tecnológica de acuerdo a las necesidades. No se tiene informe sobre el análisis de capacidades de infraestructura.

Cada 5 años se envía correo, por medio del cual se informa la renovación tecnológica a realizar, cada centro realiza el levantamiento de necesidades y el Zonal Consolida y envía a la Sede Nacional. La entrega se hace una sola entrega Se tiene una línea base única para todas las sedes, se deja en la Nube la imagen de la línea base para que cada sede sea la encargada de bajar esa imagen, siempre lo realiza una persona de TI para realizar el alistamiento.

A.8.7, Intune, Absolut, Windows Defender, Orus (Control de Instalación), ClearPass(Solo equipos institucionales). Se tienen los alertamientos pero no se están dejando las evidencias de las gestiones realizadas.

A.8.8 Se hace por medio e los correlacionados- y se tiene la sanitización frente a fallas técnicas. Garantizar que se tenga información

A.8.9 Se tiene para las herramientas adquiridas, Terminar de documentar todas las configuraciones.

A.8.10 Eliminación: No se tiene evidencia

A.8.11 Se controla por medio de información parcializada o por código de los estudiantes, Se tiene controlado en CAMPUS

A.8.12 Se hace por monitoreo de equipos por ejemplo Firewall seguimiento HOST, ClearPass, Nube Privada de la UNAD,

A.8.13 Se maneja Data Protector, se hace backup a nivel de máquina Virtual y Base de Datos y Aplicaciones. Se tienen políticas definidas, Se hace diario, retención según la máquina y contenido., siempre se hacen full, Se hace restauración por demanda se hace solicitud por correo, Se deja como evidencia los log de la máquina.

A.8.14 Se tiene en Zona Franca el Sitio Alterno.

A.8.15 Se tiene módulo de Auditoría se tiene vigencia 6 meses después de esta fecha se pasan a un backup para no generar carga transaccional. Se tiene control por terceros

A.8.16 Todos los sistemas tienen log de auditoría, se valida el SII en el cual se encuentra que no puede ser modificado, todo se tiene control no se puede modificar, se tiene acceso por la factoría.

A.8.17 Se tiene Cronos y Saturnos Se tiene VMWare, Se tiene control sobre la Hora Legal Colombia GMT-05, todas las máquinas desde allí sincronizadas.

A.8.18 Los programas utilizados en el CSIRT no son invasivos, por tal razón no son programas utilitarios, se tiene un Excel donde se tienen relacionados todos los programas. Wazuh, XDR Horus – Guardian, SW PRP, UnadSignature

A.8.19 Se hace desde el usuario administrador de la GPIT

A.8.20, A.8.21, A.8.22. Se manejan Certificados SFTP,. Se tiene 33 VLAN de acuerdo al Centro de Cableados que se tiene en la organización,
Segmentación se tiene por VLAN
Se tiene NAC para el control – ClearPass.
Todo se controla por medio autenticación en la Red.
Se tiene separa la red de Docentes, Administrativos, Finanzas, GPIT, Impresoras, Linux, VIP VoIP, todos se validan contra directorio activos

Los estudiantes y visitantes se hace autenticación por portal cautivo

Controlar el documento de Redes 2024 y generar el correspondiente etiquetado

A.8.23 Se maneja por medio de Firewall (Fortigate) por categoría y por pagina específica. Revisar el bloqueo para violencia y temas de género.

A.8.24 Se tiene canales de comunicación cifrados y lo que se tiene en la nube, las claves están cifradas se almacenas como Hash. Cada 90 días se hace cambio automático de clave, el cambio de la clave es automático

A.8.25, A.8.26, A.8.27, A.8.28, A.8.29. A.8.31. A.8.32, A.8.33 Se hace trazabilidad con el desarrollo de Compras y Presupuesto. Se tiene en el aplicativo Bitácoras.
Compras:
Se inicia con el proceso de compras de fecha 20 de junio de 2023. Se indica: Requerimiento Aplicativo Compras Iteración 2, se tienen identificados los requerimientos del desarrollo. No se tienen identificados los temas de seguridad de la información que se deben tener en cuenta. En el levantamiento de la Bitácora aparece que los riesgos son: Personal Bajo, Calendario Bajo, Negocios Bajo, Técnicos Bajo, Jurídico Bajo y Si aplica

Requerimientos legales, y en la historia de usuario aparece que solo son riesgos de calendario bajo y que no aplica requerimientos legales.
Código: Se tiene en Word, no se tiene protección del código y no se tiene etiqueta esta almacenado en la Bitácora.

Pruebas desarrollador, Pruebas QA, Pruebas de Seguridad: No se tiene evidencia de las mismas.

Pruebas de Aceptación: Se tiene evidencia de fecha 14 de Agosto de 2023.

Se revisa control de cambio para paso a producción: No se tiene

Presupuesto:
Se tiene bitácora del 12 de marzo de 2024, Riesgos: Personal Bajo, Calendario: bajo, Negocio: bajo, Técnico: Bajo, Jurídico Bajo y No Aplica requisito legales.

A.8.30 Se hace seguimiento por medio de la entrega final.

7. No conformidades

No se tienen identificados los numerales y controles aplicables a cada proceso, tal como lo solicita la norma en el numeral 5.1 (b).

No se tiene contexto de la organización documentado, incumpliendo con lo establecido en el numeral 4.1.

No se evidencia que se cuente con una matriz de partes interesadas relacionadas con seguridad de la información (necesidades y expectativas), incumpliendo con lo establecido en el numeral 4.2

No se evidencia un etiquetado y clasificación para información que está en gestión no cumpliendo con lo establecido en los controles A.5.12 y A,5,13.

No se tiene identificado el dueño del riesgo incumpliendo con lo establecido en el numeral 6.1.2 (c)

No se tienen planes para alcanzar el objetivo del Sistema de gestión de Seguridad de la información incumpliendo con el numeral 6.2

No se tiene declaración de aplicabilidad, incumpliendo con lo establecido en el numeral 6.1.3 (c)

Falta política de Continuidad y de Clasificación, incumpliendo con lo establecido en el control A.5.1

No se tiene identificados los grupos de interés especial incumpliendo con el control A.5.6

No se tiene analisis sobre la información entregada por el Csirt que permita generar inteligencia de amenazas, incumpliendo con lo establecido en el control A.5.7

No se tienen identificados los riesgos de seguridad de la información en la gestión de proyectos, tal es el caso del proyecto del DRP, incumpliendo con lo establecido en el control A.5.8

No se tiene documentada la matriz de acceso lo cual incumple con lo establecido en el control A.5.15.

No se tienen identificados riesgos de proveedores, incumpliendo con lo establecido en el control A.5.19

No se tiene plan de continuidad y el DRP está en proceso de construcción lo cual incumple con los control A.5.29 y A.5.30

No se tiene divulgación de la política de datos personales al recopilar información para el ingreso de personal. De igual forma se evidencia que se almacena por parte de uno se los funcionarios la forma del Gerente de Infraestructura. Incumpliendo de esta forma con lo establecido en el control A.5.34

No se tiene evidencia de la divulgación de la política de seguridad de la información a todas las partes interesadas incumpliendo con lo establecido en el numeral 5.2

Se tienen accesos directos en los computadores, lo cual incumple con lo establecido en el control A.7.7

No se evidencia un control adecuado sobre el filtrado WEB lo cual se soporta en que se pudo realizar navegación en Pinterest, incumpliendo con lo establecido en el control A.8.23

Se indica que el Mantenimiento UPS Se realiza una vez al año no se tiene evidencia de dicha actividad, lo cual incumple con lo establecido en el control A.7.11

No se tienen documentados los permisos que tiene cada uno de los funcionarios, incumpliendo con el control A.8.2

No se tiene informe sobre el análisis de capacidades de infraestructura, incumpliendo con lo establecido en el control A.8.6

No se evidencia un control adecuado del Código fuente, dado que se tiene almacenado en la Bitácora de los casos incumpliendo con lo establecido en el control A.8.4

No se tiene evidencia de las pruebas de seguridad. Incumpliendo con lo establecido en el control A.8.31.

No se tiene una evidencia del control de cambio para paso a producción, lo cual incumple con lo establecido en el A.8.32

Acción propuesta por parte del cliente para hacer frente a los menores incumplimientos planteados en esta auditoría:

- **N.A.**

Las no conformidades detalladas aquí se abordarán mediante el proceso de acciones correctivas de la organización, de acuerdo con los requisitos pertinentes de las acciones correctivas de la norma de auditoría, y tendrán que incluir acciones para analizar la causa de la no conformidad y prevenir que recurrente, y se mantengan los registros completos.

☐ Las acciones correctivas para hacer frente a las graves no conformidades identificadas se llevarán a cabo inmediatamente, incluyendo un análisis de las causas, y SGS notificado de las acciones adoptadas en el plazo de 30 días. Un auditor de SGS realizará una **seguimiento de la visita** en 90 días para confirmar las acciones adoptadas, evaluar su eficacia y determinar si la certificación puede otorgarse o continuar.

☐ Las acciones correctivas para abordar las graves no conformidades identificadas se llevarán a cabo inmediatamente, incluyendo un análisis de las causas, y se deberá llevar un registro con las pruebas que apoyen el envío al auditor de SGS para que el cierre se cierre en el plazo de 90 días.

☐ Las acciones correctivas para abordar los menores no conformidades identificados, incluyendo un análisis de las causas, se documentarán en un plan de acción y el cliente los enviará al auditor en el plazo de 90 días para su revisión. Si se considera que las acciones son satisfactorias, serán seguidas en la próxima visita programada.

☐ Las acciones correctivas para abordar los menores no conformidades identificados, incluyendo un análisis de las causas, han

se ha detallado en un plan de acción y la acción prevista revisada por el auditor, que se considera que es satisfactorio y se le hará un seguimiento en la próxima visita programada.

☐ Análisis de causas apropiados y acciones preventivas y correctivas inmediatas adoptadas en respuesta a cada falta de conformidad según sea necesario.

Nota:- Auditorías iniciales, de re-certificación y de extensión - recomendación para la certificación no se puede hacer a menos que se haya completado la casilla 4. Con el fin de garantizar una re-certificación, las escalas de tiempo indicadas pueden ser reducidas con el fin de garantizar una re-certificación antes de que caduca la certificación actual.

Nota: en la próxima visita a la auditoría programada, el equipo de auditorías de SGS realizará el seguimiento de *todo* identificar no conformidades para confirmar la eficacia de las medidas correctivas adoptadas.

8. Observaciones generales y Oportunidades de mejora

- Revisar y reportar mas indicadores para el SGSI.
- Relacionar todas las Entidad como contacto con autoridades.
- Garantizar la gestión completa de todos los incidentes de seguridad.
- Validar la no aplicabilidad del control A.7.10
- Garantizar el borrado seguro al devolver los equipos adquiridos por Leasing.
- Garantizar que para todos los desarrollos se realiza la identificación de los requisitos de seguridad que los mismos deben cumplir.
- Garantizar que se tenga información de fácil ubicación del análisis de vulnerabilidades
- Controlar el documento de Redes 2024 y generar el correspondiente etiquetado