Secretaría de Innovación y Desarrollo Digital/Dirección de Tecnologías de Información

Informe de Auditoría Interna

Criterios de auditoría:

Los criterios se encuentran establecidos en el DOI-011Plan Estratégico de Auditorías Internas.

Para procesos:

- Hallazgos relacionados con el proceso
- Auditorías externas realizadas recientemente o por realizar
- Quejas relacionadas

Para servicios:

- Hallazgos relacionados con el servicio
- Auditorías externas realizadas recientemente o por realizar
- Servicios próximos a certificar
- Tiempo de certificación del servicio
- Quejas relacionadas

Periodo de auditoría:

Del 09 al 11 de septiembre 2020 (se extendió hasta el 15 de septiembre).

Alcance:

Sistema de Integral de Calidad (Sistema de Administración de Calidad, Sistema de Administración de Servicios y Sistema de Administración de Seguridad de la Información).

Clasificación de hallazgos:

C: Cumple.
NC: No conformidad.
OM: Oportunidad de mejora.
N/A: No aplica.

Procesos considerados con base al Plan Estratégico de Auditorías Internas:

Proceso de Control de la Información Documentada
Proceso de Revisión Directiva
Proceso de Planeación Estratégica
Proceso de Capacitación
Proceso de Encuestas RH
Proceso de Reclutamiento y Selección
Proceso de Auditoría Interna
Proceso de Acción Correctiva
Proceso de Producto No Conforme
Proceso de Medición y Análisis

Proceso de Operaciones
Proceso del CETI
Proceso Administrativo
Subproceso de Propiedad del Usuario
Subproceso de Control Patrimonial
Subproceso de Servicios Generales
Subproceso de Ingresos y Egresos
Subproceso de Seguridad Física
Subproceso de Gestión y Ejercicio de Recursos
Subproceso de Administración de Niveles de Servicio
Subproceso de Administración de Incidentes
Subproceso de Administración de Portafolio de Servicios
Subproceso de Administración de Costos de Servicios
Subproceso Administración de la Seguridad Informática
*Subproceso de Mejora Continua
Proceso de Seguridad de la Información

Descripción de hallazgos:

No.	Alcance	Clasificación del hallazgo	Requisito	Descripción del Hallazgo	Folio de Acción Correctiva
1	ISO 9001:2015	NC	7.2 d)	**Requisito incumplido:** La organización debe: d) conservar la información documentada apropiada como evidencia de la competencia. **Hallazgo encontrado**: Durante la auditoría interna se revisó el proceso de capacitación, el cual establece que se llevan a cabo cursos para el personal de la DTI, al momento de solicitar información del curso Desarrollo de Personas no se muestran las evaluaciones del curso del total de los asistentes, así como del curso Políticas de Seguridad en donde no se mostró la verificación de la efectividad, siendo que se impartió desde el mes de Febrero y el proceso establece que la verificación es 3 meses después de la impartición. **Evidencia objetiva:** PG-06-001 Proceso de Capacitación, ID 224 Curso de Desarrollo de Personas, ID 223 Políticas de Seguridad.	09-01/20

No.	Alcance	Clasificación del hallazgo	Requisito	Descripción del Hallazgo	Folio de Acción Correctiva
2	ISO 27001:2013	NC	**A 10.1.1** Política en el uso de controles criptográficos	**Requerimiento incumplido**: Se debe desarrollar e implementar una política sobre los controles criptográficos para la protección de la información. **Hallazgo encontrado**: Durante la auditoría interna se revisó si los equipos de cómputo estaban cifrados. Y de los cuales no se pudo mostrar la evidencia de su aplicación. **Evidencia que soporta la no conformidad:** DOI-156 Política de Controles criptográficos	09-02/20
3	ISO 27001:2013	NC	**A 12.4.2** Protección de registros de información	**Requerimiento incumplido**: Los dispositivos de registro y los registros de información deben ser protegidos contra manipulación y acceso no autorizado. **Hallazgo encontrado**: si bien se presentó evidencia que guardaba los Logs en cada sistema, no se pudo mostrar evidencia que apoye a proteger contra cambios o eliminación no autorizados de los Logs y la manera en que se salvaguardan. **Evidencia que soporta la no conformidad:** Logs de los sistemas	09-03/20
4	ISO 9001:2015	OM	8.1 Planificación y control operacional	**Hallazgo encontrado**. Durante la auditoría interna se revisa el proceso de planeación estratégica, el cual establece que para todas las iniciativas nuevas deben establecerse el/los objetivos de calidad en el cual impacta dicha iniciativa, y se validan las del 2020 y todas tienen referencia a un objetivo, sin embargo, en una iniciativa derivada de un seguimiento el área está pendiente de entregar esa información, por lo que, es necesario afianzarla desde el momento que se crea. **Evidencia objetiva:** Iniciativa 4, del seguimiento a la PE Junio 2020.	No aplica

No.	Alcance	Clasificación del hallazgo	Requisito	Descripción del Hallazgo	Folio de Acción Correctiva
5	ISO 27001:2013.	OM	8.2	**Hallazgo encontrado**: Durante la auditoría interna se revisó el RC-04-027 Evaluación y Tratamiento de Riesgos, en donde se consideran todos los activos críticos derivados del Inventario de Activos, no se puede identificar claramente los activos que no tienen control asociado y de los que tienen control no se percibe la revisión de que efectivamente se están llevando a cabo y son efectivos. **Evidencia objetiva:** RC-04-027 Evaluación y Tratamiento de Riesgos.	No aplica
6	ISO 27001:2013.	OM	9.1	**Hallazgo encontrado:** Durante la auditoría interna se revisa el indicador del proceso de seguridad, el cual se está midiendo considerando la revisión de 25 controles que son los que se implementan por personal de la DTI, sin embargo, se podría hacer el análisis para saber si se puede incrementar la cantidad de controles, sobre todo ahora que no hay personal físicamente en el edificio y no pueden validarse los 25 considerados. **Evidencia objetiva**: Registro de auditorías aleatorias.	No aplica
7	ISO 27001:2013	OM	**A9.1.1** Política de control de acceso	**Hallazgo encontrado**: Durante la auditoría interna, se detecta que si bien si se define los privilegios de los accesos a los activos con los usuarios, no se valida la frecuencia definida de la vigencia en los accesos a los usuarios definido en la política **Evidencia que soporta la mejora:** Se mostró el folio 93701 en donde se solicitaba otorgar permisos de acceso a la Base de Datos de KAIZEN, en donde se especificó qué nivel de privilegios	No aplica

No.	Alcance	Clasificación del hallazgo	Requisito	Descripción del Hallazgo	Folio de Acción Correctiva
8	ISO 27001:2013	OM	**A9.4.1** Restricción de acceso a la información	**Hallazgo encontrado**: Durante la auditoría interna, se mostró la identificación y autentificación de los usuarios, pero en la política se especifica ciertas políticas a seguir referente a las contraseñas que no se aplican. **Evidencia que soporta la mejora:** Se presentó el siguiente folio 96405 el cual se solicitaba que se otorgara el permiso de acceso al servidor de digitalización para un conjunto de IP's.	No aplica
9	ISO 27001:2013	OM	**A9.4.2** Procedimientos de inicio de sesión seguro	**Hallazgo encontrado**: Durante la auditoría interna, se detecta que si bien se presentó evidencia de la obtención de los registros de Log on, log off, log fail, no se le está dando seguimiento a la correlación de información obtenida, lo que hace que no se pueda detectar a tiempo posibles incidentes **Evidencia que soporta la mejora:** Se mostró el sistema web ciati.uanl.mx como evidencia de inicio seguro, también se mostró una solicitud de CIATI número 96966 con la descripción acceso BD Nexus para el seguimiento en un acceso a través de una VPN que ya manejaba el solicitante.	No aplica
10	ISO 27001:2013	OM	**A11.1.5** Trabajo en áreas seguras	**Hallazgo encontrado**: Durante la auditoría interna, se detecta que algunos lineamientos no se están siguiendo a forma solicitada por el documento DOI-126 como por ejemplo la política #14. **Evidencia que soporta la mejora:** Se mostró el documento DOI-126 lineamientos de trabajo en el centro de telecomunicaciones y área de servidores del centro de cómputo con revisión 00-06/19, también se comentó del listado de visitantes RC-ADM-06-031	No aplica

No.	Alcance	Clasificación del hallazgo	Requisito	Descripción del Hallazgo	Folio de Acción Correctiva
11	ISO 27001:2013	OM	**A 12.6.1** Gestión de vulnerabilidades técnicas	**Hallazgo encontrado**: Durante la auditoría interna, se detecta que la organización utiliza varias herramientas para identificar las vulnerabilidades en los sistemas, pero no se le da seguimiento a los hallazgos que presentan las herramientas. **Evidencia que soporta la mejora:** Se mostró las herramientas que se utiliza para la identificación de vulnerabilidades. nmap, zap proxy, wpscan y openvas	No aplica
12	ISO 20000:2018	OM	7.5.2 c)	**Hallazgo encontrado**: Durante la auditoría se detectó que se actualizó el documento colocándose la etiqueta de seguridad, con Rev. 05-02/20 y de acuerdo a la fecha de solicitud de esta actividad debe de ser Rev. 05-09/20 **Evidencia objetiva:** SP-SER-019 Subproceso de Administración de Seguridad de la Información	No aplica

Resumen de hallazgos:

Alcance	Cantidad	Proceso/subproceso o control relacionado:	Total
ISO 9001:2015	1 NC	Capacitación	**3**
ISO 27001:2013	2 NC	Control de seguridad de criptografía Control de seguridad de protección de registros de información	
ISO 9001:2015	1 OM	Planeación Estratégica	**9**
ISO 20000:2018	1 OM	Seguridad de la Información	
ISO 27001:2013	7 OM	Controles varios	

Firmas de aprobación

Auditor Líder	**Representante de Dirección de ISO9001**	**Director**