



DPHIR SAS



Explicación Sistema de Información de Votaciones de la UNAD



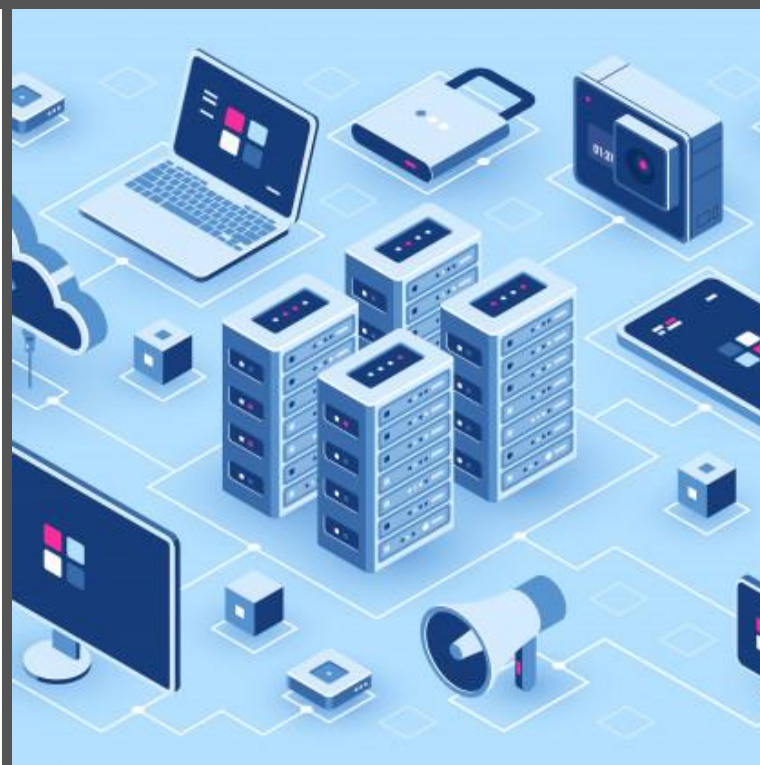
Evaluación seguridad informática Sistema Información de Votaciones UNAD



Aseguramiento de códigos fuentes
– Inscripción y Consulta–



Aseguramiento de bases de datos
– Inscripción y Consulta–



CONTEXTUALIZACIÓN

Sistema Nacional de Elecciones - UNAD





Contextualización

De acuerdo con la orden de servicio identificada como OS-2022-000039 de fecha doce (12) de agosto de dos mil veintidós (2022), se define el objeto de esta auditoría:



Objeto Auditoría
Forense

Prestar el servicio de auditoría en seguridad de la información al sistema de elecciones nacionales de la UNAD y su base de datos, dentro del proceso participativo que se adelanta para la designación de rector de la universidad, de conformidad con las resoluciones y acuerdos que reglamenten los procesos, realizando el respectivo acompañamiento para el aseguramiento y certificación de las bases de datos (estampas cronológica).



Sistema Nacional
de Elecciones

El sistema Nacional de Elecciones de la Universidad Nacional Abierta y a Distancia, basados en la utilización de herramientas de TI, permite realizar procesos de participación ciudadana de manera digital, permitiendo la invitación de los diferentes estamentos de este claustro universitario en procesos electorales que se llevan en esta.

El Sistema Nacional de elecciones implementado por la UNAD esta desarrollado bajo una arquitectura de software denominada MVC (modelo, vista, controlador), la cual permite separar los datos de una aplicación, la interfaz de usuario, y la lógica de control.



Evaluación de Seguridad

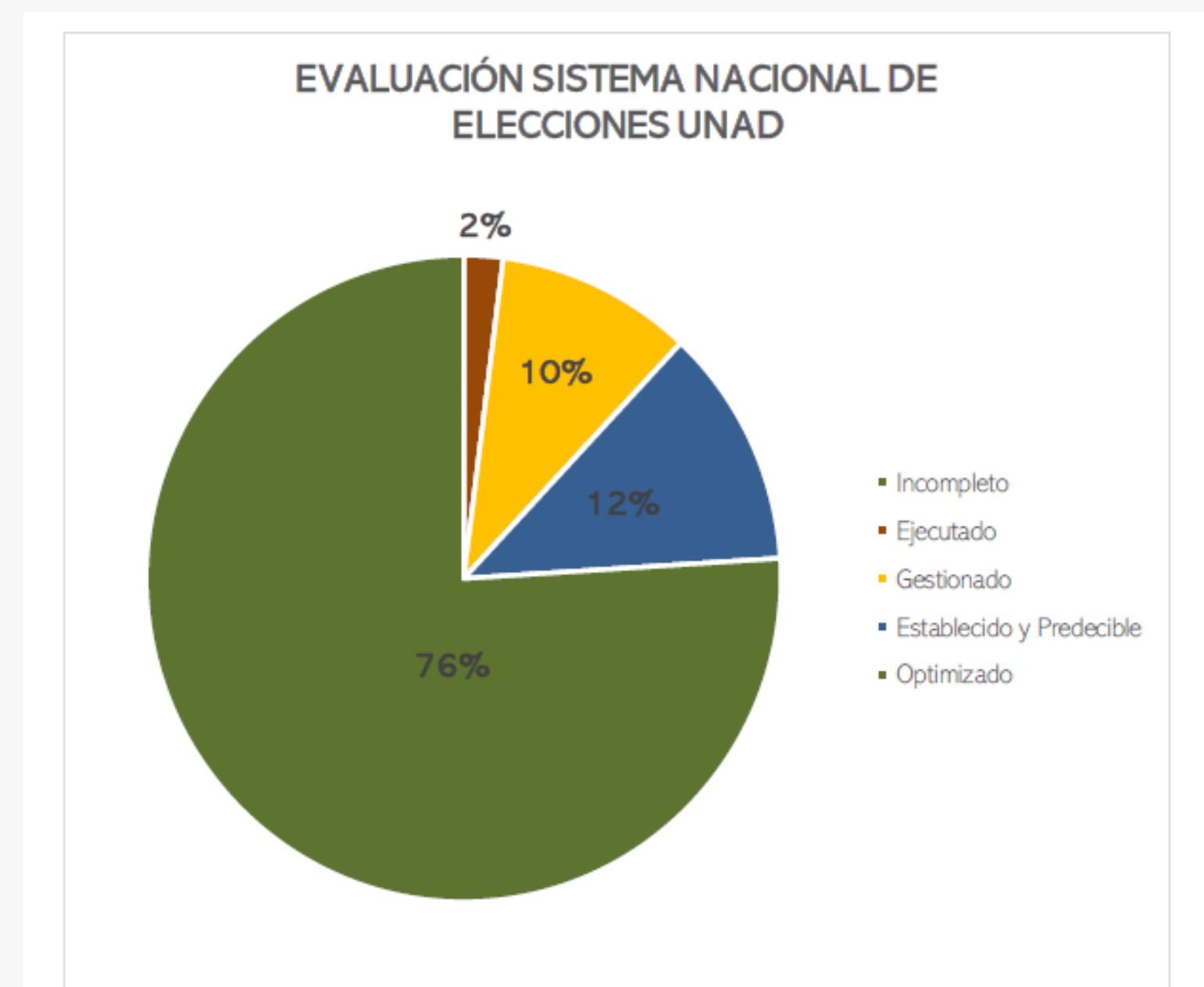
Sistema Nacional de Elecciones UNAD



Análisis de Seguridad

Se hizo un análisis de seguridad de la información y ciberseguridad frente a los controles implementados por la UNAD en su Sistema Nacional de Elecciones, tomando como referencia la norma ISO 27001:2013 - Anexo A -, evaluando 59 controles, arrojando los siguientes resultados:

ESTADO	DEFINICIÓN	PORCENTAJES CONTROLES
Incompleto	Ausencia total o muy poca evidencia de política reconocible, procedimiento, control, etc.	0%
Ejecutado	Progresando muy bien, el proceso alcanza su propósito, pero todavía no se completa	2%
Gestionado	El proceso anteriormente descrito está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados descritos.	10%
Establecido y Predecible	El desarrollo es completo, el proceso/control se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.	12%
Optimizado	El requisito es completamente satisfecho, está operando plenamente como era de esperarse, se está monitoreando y mejorando de forma continua para cumplir con las metas empresariales presentes y futuras, y hay pruebas sustanciales para probar todo a los auditores	76%
TOTAL		100%



Para mencionar ...

Frente a temas de ciberseguridad se quieren mencionar los siguientes aspectos:

Votación

Participativo;
Secreto;
Individual;
Una sola vez.

Seguridad de la Información

Segmentación de Responsabilidades;
Un solo administrador de la Plataforma de Elecciones;
Cifrado de contraseña de autenticación.;
Servicio Proctering;
Log de seguridad del sistema Nacional de Elecciones.;
Backups;
Procedimiento de Administración de Incidentes de seguridad.

Seguridad Informática

Firewall;
VLAN;
CSIRT Institucional;
Datacenter (Tier IV);
Herramientas de antivirus;
Plataforma de Continuidad del servicio;
Servicios web seguros.

Conclusión N 1

El Sistema Nacional de Elecciones de la *Universidad Nacional Abierta y a Distancia* cumple adecuadamente con niveles de seguridad de la información, informática y ciberseguridad, esto, frente a los controles evaluados con ocasión de la protección de los datos de la consulta pública no vinculante para la elección de rector, permitiendo con ello, asegurar la integridad, confidencialidad, disponibilidad, seguridad, no repudio, autenticidad, mismidad y legalidad de los datos que aquí se recaudaron



ASEGURAMIENTO
FORENSE

Aseguramiento Forense

Con ocasión de la auditoria forense realizada se ejecutaron las siguientes actividades:

Aseguramiento Inicial del Código Fuente del programa de Elecciones

Se aseguro el código fuente del programa que gestiona el Sistema Nacional de Elecciones para el proceso de inscripción de candidatos, así como para la consulta de rector no vinculante al momento de iniciar cada uno de estos procesos.

Aseguramiento Final del Código Fuente del programa de Elecciones

Al finalizar cada uno de estos procesos, es decir, inscripción de candidatos y consulta no vinculante de rector, se aseguro el código fuente comparándolo con el aseguramiento inicial, siendo estos coincidentes, y con ello, se logró demostrar su autenticidad

Revisión de bases de datos con contadores en cero

Se revisaron las bases de datos del Sistema Nacional de Elecciones al inicio de la consulta de rector no vinculante, verificando que sus contadores estuvieran en cero (0).

Aseguramiento de la base de datos de elecciones diariamente.

Durante todo el proceso de las votaciones, se aseguro la base de datos y el código fuentes de la aplicación diariamente extrayendo dos (2) copias.

Conclusión N 2

Dentro del proceso de auditoria desarrollado por DPHIR®, se hizo una comparación de los archivos que hacen parte del código fuente del aplicativo de elecciones, encontrando que estos son exactamente iguales en los diferentes momentos en los cuales se extrajo la copia binaria, esto es, los días treinta (30) de agosto y ocho (8) de octubre de dos mil veintidós (2022), demostrando con ello, que el código fuente no sufrió modificaciones durante el desarrollo de las elecciones, cumpliendo con la funcionalidad para la que fue desarrollado

Frente al Aseguramiento de las Bases de Datos





Auditoria Forense

Como mecanismo de aseguramiento del Sistema Nacional de Elecciones de la UNAD, al momento de iniciar este proceso fueron asegurados los repositorios de información electoral, esto es, la base de datos, y a partir de allí, se aseguraron diariamente cada uno de los *Backups* de estos repositorios, obteniendo 90 copias de las base de datos entre el 16 y el 22 de agosto de 2022 para el caso de inscripción de candidatos, y el 31 de agosto al 7 de octubre de 2022 para la consulta no vinculante.

Estampa de Tiempo

A través de un reloj atómico se extrajo la fecha y hora legal de cuando se obtuvo cada imagen forense

Extracción de HASH

Se identificó cada imagen forense con un código único inmodificable

Imagen Forense

Extrajo una copia exacta y protegida de la base de datos de elecciones diariamente.

01

02

03

Conclusión 3

Los profesionales de DPHIR® realizaron el aseguramiento de cincuenta (50) imágenes forenses, en las cuales se encuentran noventa (90) copias de la base de datos de elecciones en diferentes instantes de tiempo, por ende, estas copias forenses podrán ser tomados como prueba digital, en caso de así requerirlo, ya que estas **NO PUEDE SER MODIFICADAS** a partir del momento de su recaudo, manteniendo así, características de mismidad, autenticidad, trazabilidad y auditabilidad..

Evidencias

Como evidencias de este proceso se tienen:

Backup de la Base
de Datos

Imagen Forense

Estampa Tiempo

Certificación

Acta de
Intervención

A través de las actividades realizadas y definidas por la Universidad, es posible hacer un seguimiento posterior a esta consulta pública virtual no vinculante para la elección del rector, pudiendo ser verificada por organismos de control en caso de requerirse, salvaguardando con ello, características de auditabilidad y reproducibilidad.



John Jairo Echeverry Aristizabal



DPHIR SAS



facebook.com



twitter.com



johnjairo@dphir.co



+57 3142495534

DPHIR SAS