INCIDENCIA A CAUSA DE ATAQUES DE CIBERSEGURIDAD

SISTEMA DE REPRESENTANTES DE PARTIDOS POLÍTICOS Y CANDIDATURAS INDEPENDIENTES

Unidad Técnica de Servicios de Informática

CONTROL DE VERSIONES

VERSIÓN	COMENTARIO / DESCRIPCIÓN	RESPONSABLE DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN	FECHA DE ACTUALIZACIÓN / CREACIÓN / REVISIÓN
1.0	Creación del Documento	Diana Tapia Campos	16/04/2018
1.1	Actualización del Documento	José Carmen Hernández Padrón	31/01/2020

AUTORIZACIONES Y RESPONSABLES

Responsables de la aprobación, revisión y elaboración del presente documento.

ELABORÓ:

FECHA	PUESTO	ÁREA	NOMBRE Y FIRMA
31/01/2020	Jefe de Departamento de Análisis de Riesgos	Unidad Técnica de Servicios de Informática	José Carmen Hernández Padrón

REVISÓ:

FECHA	PUESTO	ÁREA	NOMBRE Y FIRMA
04/02/2020	Subdirectora de Seguridad Informática	Unidad Técnica de Servicios de Informática	Lissette Morones Sánchez

APROBÓ:

FECHA	PUESTO	ÁREA	NOMBRE, FIRMA Y RUBRICA
04/02/2020	Director de Seguridad y Control Informático	Unidad Técnica de Servicios de Informática	Yuri Adrián González Robles

Contenido

Glosario

Activo	Cualquier ente tangible o intangible que tiene valor para el Instituto y que requiere protección. Existen muchos tipos de activos, incluyendo: a) Activos de información: bases de datos y archivos de datos, hojas electrónicas con datos, contratos y acuerdos, documentación del sistema, información de investigaciones, manuales de usuario, material de capacitación, procedimientos operacionales o de soporte, acuerdos para contingencias, rastros de auditoría e información archivada. b) Activos de software: software de aplicación, software del sistema, herramientas de desarrollo. c) Activos físicos: equipo de cómputo, equipo de comunicación, medios removibles y otros equipos. d) Servicios: servicios de computación y comunicación, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado. e) Personas: competencias, habilidades, experiencia y los roles que desempeñan. f) Intangibles: tales como la reputación y la imagen del Instituto.
Ataque Informático	Es un intento o maniobra ofensiva mediante un sistema informático con la finalidad de afectar a un sistema informático o red; intenta tomar control, desestabilizar o dañar otro sistema.
CCO	Centro de Cómputo y Operaciones.
Ciberseguridad	La ciberseguridad busca proteger la información digital través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.
Cross-Site Scripting	Es un ataque que busca las vulnerabilidades en una aplicación web para realizar inyección de código malicioso mediante un script, el cual se presenta en forma de hipervínculo para conducir al usuario a otro sitio web, con la finalidad de robar información sensible, secuestrar sesiones de usuario y comprometer al navegador.
Defacement	Es un ataque a un sitio web donde se toma el control del mismo y se modifica la apariencia visual, contenido o configuración de un sitio web, ya sea total o parcial, sin autorización.
DOR	Departamento de Operación de Redes
DoS	Ataque de Denegación de servicio. Consiste en generar una cantidad masiva de peticiones al servidor, provocando así una sobrecarga del mismo, alterando el servicio.

Incidente de seguridad de la información	Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información.
Instituto	Instituto Nacional Electoral.
Phishing	Es un ataque conocido como suplantación de identidad. Es un método utilizado para conseguir que se revele información personal, consiste en el envío de correos electrónicos que aparentan provenir de fuentes confiables e intentan obtener datos confidenciales del usuario, pueden ser utilizadas para ejecutar algún tipo de fraude.
Plan de continuidad	Mecanismo de respuesta a incidentes de control de crisis que permitan la continuidad de las operaciones, en caso de que se presenten casos fortuitos o de fuerza mayor.
Ransomware	Es un ataque que causa un secuestro exprés de datos, restringiendo el acceso al sistema, cifrando la información obtenida y exigiendo un rescate para liberarla.
Servicio en la Nube	Servicios que utilizamos y no se encuentran físicamente instalados en el equipo. La forma de acceder a estos servicios es mediante internet.
Sistemas de Información	Están compuestos por aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la información y ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información.
SOC	Centro de Operaciones de Seguridad.
WAF	Firewall de Aplicación Web. Es un tipo de firewall que se utiliza para controlar el acceso a una aplicación o servicio web. A diferencia de un firewall tradicional, este opera sobre la capa de aplicación (capa 7 del modelo OSI), por lo que es posible considerar algunos controles de seguridad más robustos.

1. Objetivo

El objetivo del presente documento es llevar a cabo un análisis de los posibles incidentes a causa de ataques de ciberseguridad, centrándose en la operación de la infraestructura que da soporte al Sistema de Representantes de Partidos Políticos y Candidatos Independientes, a fin de mitigar el impacto en la operación del mismo ante posibles incidentes que se presenten.

Asimismo, se ha seguido una planeación basada en el análisis de escenarios adversos o de contingencia y se han tomado las medidas necesarias que permitirán garantizar un tiempo óptimo de recuperación y un impacto mínimo en el funcionamiento general de los sistemas informáticos.

Adicionalmente se busca dar a conocer las acciones a realizar en caso de que se presente algún incidente por ataques de ciberseguridad, tal como Denegación de servicio (DoS), Cross-Site Scripting (XSS), Defacement, Phising, SQL injection, XML External Entities (XXE), exposición de datos sensibles del servicio web, ataques de diccionario y ataques de fuerza bruta.

2. Escenarios

2.1. Identificación y atención de ataques de Ciberseguridad

Número	Herramienta	Actividad
1	Herramienta para la protección contra ataques de denegación de servicio en sitio.	Enviar cada hora el análisis del tráfico del grupo de protección **Representantes** al grupo de **Telegram** del Departamento de Auditoría Informática.
2	Firewall de aplicaciones web.	Enviar cada hora el análisis de las alertas del sistema al grupo de **Telegram** del Departamento de Auditoría Informática.
3	Herramienta para la protección contra ataques de denegación de servicio en la nube.	Enviar cada hora el análisis del tráfico del sistema al grupo de **Telegram** del Departamento de Auditoría Informática.
4	Herramienta de monitoreo de red.	Solicitar al SOC un reporte de todos los eventos identificados para los nodos y balanceador del sistema**.** Enviar cada hora el análisis del tráfico al grupo de **Telegram** del Departamento de Auditoría Informática.

2.2. Incidencia en el Sitio Web de Sistema de Representantes

Herramienta	Actividad	Recursos
Herramienta para la protección contra ataques de denegación de servicio en sitio.	En caso de identificar tráfico anómalo en el Sistema de Representantes se deberá proceder conforme lo siguiente:	• Grupo de Whatsapp de Atención de Reglas de Firewall.

Herramienta	Actividad	Recursos
	1.- Identificar que el umbral sea mayor al definido. 2.- Solicitar la aplicación de la mitigación al SOC. 3.-Notificar al personal del Departamento de Operación de Redes, vía WhatsApp, solicitando su apoyo para validación. 4.- Notificar en el Grupo de WhatsApp "Sistema de Representantes INE", solicitando su apoyo para validación.	• Grupo de Whatsapp de "Sistema de Representantes INE". • Correo electrónico y números telefónicos del SOC.
Firewall de aplicaciones web	En caso de identificar una alerta de impacto alto se deberá proceder conforme lo siguiente: 1.- Identificar que el ataque haya sido bloqueado por la herramienta. Aparecerá el siguiente icono: ⛔ . 2.- Identificar la IP del origen del ataque. 3.- Solicitar el bloqueo de las IP al Departamento de Operación de Redes vía WhatsApp. 4.- Solicitar apoyo del SOC vía correo electrónico y llamada telefónica.	• Grupo de Whatsapp de Atención de Reglas de Firewall. • Grupo de Whatsapp de Sistema de Representantes INE. • Correo electrónico y número telefónico de SOC.
Herramienta para la protección contra ataques de denegación de servicio en la nube.	En caso de identificar tráfico anómalo se deberá proceder conforme lo siguiente: 1.-Notificar al personal del Departamento de Operación de Redes vía WhatsApp solicitando su apoyo para validación. 2.- Notificar en el Grupo de WhatsApp "Sistema de Representantes INE", solicitando su apoyo para validación.	• Grupo de Whatsapp de Atención de Reglas de Firewall. • Grupo de Whatsapp de "Sistema de Representantes INE".
Herramienta de monitoreo de red.	En caso de identificar algún comportamiento del tráfico anómalo se deberá proceder conforme lo siguiente: 1.-Notificar al personal del Departamento de Operación de Redes, vía WhatsApp solicitando su apoyo para validación de IP y en su caso bloqueo de la misma. 2.- Notificar en el Grupo de WhatsApp "Sistema de Representantes INE", solicitando su apoyo para validación.	• Grupo de Whatsapp de Atención de Reglas de Firewall. • Grupo de Whatsapp de "Sistema de Representantes INE".

2.3. Incidencia por Phishing

Número	Responsable	Actividad
1	Subdirección de Seguridad Informática	Analiza la información respecto al sitio reportado/detectado como falso.
2	Subdirección de Seguridad Informática	Si se cuenta con algún correo electrónico utilizado para esparcir el sitio malicioso, solicitar al área usuaria la cabecera del correo para determinar su origen. Si el usuario no conoce la manera en que se obtiene la información, es asesorado por personal de Seguridad.
3	Subdirección de Seguridad Informática	Determina si el sitio phishing se encuentra activo al acceder a la URL maliciosa. Plasma la información recabada en el formato de Reporte de Incidentes.
4	Subdirección de Seguridad Informática	Determina el origen de la dirección IP, de no pertenecer al Instituto se deberá consultar en los registros de Internet Regionales (RIR) que sean responsables de asignar y registrar direcciones IP en Internet (ARIN, RIPE, APNIC, AFRINIC, LACNIC, entre otros), para notificar al responsable sobre el incidente. La notificación se realizará mediante correo electrónico y será enviada a los contactos abuse@ que se encuentren registrados, puede usarse el sitio (http://centralops.net/co/) para obtener esta información. Adicionalmente será enviado un correo para notificar el incidente a los CERT´s nacionales para que puedan apoyar en la denuncia del incidente. UNAM-CERT: incidentes@seguridad.unam.mx CERT-MX: cert-mx@ssp.gob.mx Si es posible determinar el origen de los correos maliciosos notificar al administrador del sitio.
5	Subdirección de Seguridad Informática	En caso de que se detecte que la IP provenga de equipos en la red del INE, se procederá a documentar las direcciones IP que estén relacionados con el incidente.
6	Subdirección de Seguridad Informática	En conjunto con el área usuaria determinar si el bloqueo del tráfico de red del servicio web de la IP involucrada afecta el funcionamiento del sistema.
7	Subdirección de Seguridad Informática	Los equipos cuyas direcciones IP estén implicadas en casos de sitios phishing y que pertenezcan a la RedINE, deberán ser revisadas con base en el procedimiento: “**Manejo de código malicioso**”.

Número	Responsable	Actividad
8	Subdirección de Seguridad Informática	Si se determina que es posible bloquear el tráfico de red, tanto interno como externo, solicita al personal del Departamento de Operación de Redes que proceda al bloqueo de los puertos. El bloqueo se debe aplicar en los dispositivos que se consideren necesarios, hasta que se remuevan los archivos del sitio falso del servidor. **Nota:** En caso de contar con "Servicios Administrados por terceros" notificar por correo electrónico y llamada telefónica.
9	Subdirección de Seguridad Informática Departamento de Operación de Redes	En caso de contingencia y que ninguno de los pasos anteriores ayude a contener el problema, se debe analizar la opción de poder modificar la dirección IP de los equipos que están siendo atacados.
10	Subdirección de Seguridad Informática	Solicita a personal del Departamento de Operación de Redes que proceda a capturar el tráfico entrante y saliente del equipo afectado.
11	Subdirección de Seguridad Informática	En conjunto con el Departamento de Operación de Redes realizaran el análisis correspondiente tratando de identificar patrones relacionados con algún ataque ya conocido o publicado en Internet.
12	Subdirección de Seguridad Informática Departamento de Operación de Redes	Identifica vulnerabilidades o servicios mal configurados.
13	Subdirección de Seguridad Informática Departamento de Operación de Redes	Corrige las vulnerabilidades o servicios mal configurados identificados.
14	Subdirección de Seguridad Informática	Genera un reporte incluyendo la evidencia del incidente presentado.

2.4. Manejo de Código Malicioso

Número	Responsable	Actividad
1	Subdirección de Seguridad Informática	En caso de ser posible presta soporte vía telefónica. De lo contrario acudir al área donde se ubica el equipo afectado por código malicioso.
2	Subdirección de Seguridad Informática	Con apoyo del responsable del equipo identifica los incidentes de seguridad y solicita una descripción del incidente.
3	Subdirección de Seguridad Informática	En caso de corroborar que se presenta una infección por código malicioso realizar una evaluación técnica del estado del equipo afectado, determina si es necesario desconectar el equipo de la red o apagar el equipo infectado para evitar que el virus/gusano informático se propague a otros equipos.
4	Subdirección de Seguridad Informática	Lleva un registro de las acciones tomadas.
5	Subdirección de Seguridad Informática	Da aviso a las áreas correspondientes de la evaluación técnica del estado del equipo.
6	Subdirección de Seguridad Informática	En caso de no corresponder a un incidente por código malicioso determina en conjunto con el área usuaria la correcta clasificación del incidente: • Robo de equipo • Acceso no autorizado físico o lógico • Penetración al sistema • Modificación de página Web • Sabotaje • Mal uso de las aplicaciones públicas en el sitio
7	Subdirección de Seguridad Informática Departamento de Operación de Redes	Verifica con el Departamento de Operación de Redes, si es posible que aísle el equipo con acceso exclusivo a las rutas del Antivirus en el servidor que corresponda, según el área a la que pertenece el usuario que tiene en ese momento el incidente de código malicioso y de ser así proceder al asilamiento.
8	Subdirección de Seguridad Informática	Solicita al área usuaria que encienda el equipo y que habilité una sesión con el usuario Administrador o su equivalente.
9	Subdirección de Seguridad Informática	Identifica si el equipo cuenta con el cliente del antivirus institucional instalado.
10	Subdirección de Seguridad Informática	Si no se cuenta con el cliente de antivirus institucional, procede a instalarlo desde el servidor que quedo accesible para el equipo.
11	Subdirección de Seguridad Informática	Identifica si el cliente del antivirus institucional cuenta con las últimas actualizaciones.
12	Subdirección de Seguridad Informática	Si el cliente está desactualizado, espera a la actualización automática del antivirus institucional.
13	Subdirección de Seguridad Informática	Ejecuta el antivirus institucional, para determinar el virus/gusano que está afectando al equipo en cuestión.

Número	Responsable	Actividad
14	Subdirección de Seguridad Informática	Trata de eliminar automáticamente el código malicioso que afecta al equipo.
15	Subdirección de Seguridad Informática	En caso de no poder eliminar el virus, busca si existe alguna herramienta de erradicación del virus en el sitio oficial del proveedor de antivirus.
16	Subdirección de Seguridad Informática	Coloca dicha herramienta dentro de los límites definidos por el Departamento de Operación de Redes.
17	Subdirección de Seguridad Informática	Si se encontró dicha herramienta, la pone en funcionamiento de acuerdo con el instructivo de la página del proveedor.
18	Subdirección de Seguridad Informática	Elimina todos los archivos relacionados al código malicioso y efectúa limpieza de registro de Windows.
19	Subdirección de Seguridad Informática	En caso de no poder eliminar algún archivo de programa o de sistema operativo, será necesario canalizar el equipo al área de soporte para la reinstalación de los programas o del sistema operativo.
20	Subdirección de Seguridad Informática	Realiza una inspección de los procesos del sistema, utilizando la aplicación “taskmgr.exe” y “Security Task Manager” y determinar si existe algún procedimiento no común a las tareas que normales de la operación.
21	Subdirección de Seguridad Informática	En caso de encontrar el archivo malicioso en el equipo infectado, accede al sitio (https://www.virustotal.com/es/) para subir la muestra y saber si otros motores antivirus lo reconocen.
22	Subdirección de Seguridad Informática	Realiza una inspección de las llaves del registro del sistema operativo utilizando la aplicación “regedit.exe”. Examina y restaura las llaves del registro que son utilizadas comúnmente por los virus/gusanos informáticos. Apoyándose en información publicada en el sitio del proveedor del Antivirus Institucional. (En este punto se hace hincapié en revisar la clave “run”). Es importante recordar que cualquier cambio erróneo puede suponer la pérdida de funcionalidad del equipo de cómputo.
23	Subdirección de Seguridad Informática	Realiza una inspección de los puertos de comunicación TCP que están activos en el equipo haciendo uso de la herramienta “fport.exe” y “netstat.exe”. Determina los puertos que están asociados a actividad del código malicioso. Determina qué proceso está asociado a los puertos identificados y procede a eliminarlos.
24	Subdirección de Seguridad Informática	Realiza una búsqueda de código malicioso, ejecutando el cliente del antivirus Institucional. Si el reporte del antivirus no arroja ninguna anormalidad, procede a cerrar el incidente generando el respectivo informe.

2.5. Identificación y Contención de ataques tipo Defacement, Cross-Site Scripting (XSS), Phising, SQL injection, XML External Entities (XXE), exposición de datos sensibles del servicio web, ataques de diccionario y ataques de fuerza bruta

Número	Responsable	Actividad
1	Subdirección de Seguridad Informática	Acude al sitio donde se ubica físicamente el equipo afectado por el incidente, en compañía del área responsable del equipo.
2	Subdirección de Seguridad Informática	Realiza una evaluación técnica del estado del equipo afectado.
3	Subdirección de Seguridad Informática	Determina si es necesario tomar acciones adicionales para evitar que se tome control del equipo afectado.
4	Subdirección de Seguridad Informática	Determina si es necesario tomar acciones adicionales para dar solución al incidente o si es suficiente con las acciones aplicadas por el usuario previamente.
5	Subdirección de Seguridad Informática	Lleva un registro de las acciones tomadas.
6	Subdirección de Seguridad Informática	Con el apoyo del responsable del equipo afectado identifica a los administradores del equipo y les notifica el incidente.
7	Responsable del Sistema o equipo afectado	Se hacen la modificaciones y validaciones pertinentes y si se cuenta con un respaldo del sitio web, da de baja el equipo comprometido y poner en línea el backup.
8	Subdirección de Seguridad Informática	Monitorea el respaldo en línea para identificar y contener alguna nueva modificación.
9	Subdirección de Seguridad Informática Departamento de Operación de Redes	Solicita a personal del Departamento de Operación de Redes que proceda a capturar el tráfico entrante y saliente del equipo en línea.
10	Subdirección de Seguridad Informática Departamento de Operación de Redes	Si no se cuenta con algún soporte de respaldo, determina si es posible bloquear el tráfico de red, tanto interno como externo y solicita a personal del Departamento de Operación de Redes que proceda al bloqueo de los puertos. El bloqueo se debe aplicar en los dispositivos que se consideren necesarios, hasta que se remuevan los archivos modificados en el servidor.
11	Subdirección de Seguridad Informática	Revisa el equipo comprometido con base en el procedimiento denominado: “**Manejo de código malicioso**”.
12	Subdirección de Seguridad Informática	Si se ha solucionado el incidente, genera el reporte de incidentes indicando las acciones tomadas al momento.