ITESCA®
Instituto Tecnológico Superior de Cajeme

PLAN PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA V 1.1

SONORA
TIERRA DE OPORTUNIDADES

Contenido

1. HISTORIAL DE VERSIONES

FECHA	REVISIÓN	AUTOR	VERIFICADO POR
04/11/2024	1.1	Mtra. Norma Lilia Saucedo Ocha	Ing. Tadrio eugenio Teran Serrano
		M.I. Eduardo Ignacio Urbalejo Rios	
		Ing. Tadrio Eugenio Teran Serrano	

2. DOCUMENTO VALIDADO POR LAS PARTES EN FECHA:

DIRECCION GENERAL DE INFRAESTRUCTURA TECNOLOGICA Y CONECTIVIDAD		
POR LA SUBDIRECCIÓN	**POR LA DIRECCIÓN**	**POR LA DIRECCION GENERAL**

1. INTRODUCCION

El presente documento tiene por objetivo generar un esquema de acciones que permita preservar la información y asegurar la continuidad de los servicios esenciales del Instituto Tecnológico Superior de Cajeme, en el menor tiempo posible, ante la ocurrencia de un incidente de seguridad informática, minimizando su impacto.

2. PROPOSITO

IDENTIFICACION DEL REQUERIMIENTO:	RF-01
NOMBRE DEL REQUERIMIENTO:	Plan de Acción para Incidentes de Seguridad Informática.
REFERENCIA:	Basado en el Boletín Oficial del Estado de Sonora, Tomo CCXIV, Número 16 Secc. II (22 de agosto de 2024)
CARACTERISTICAS DEL PLAN:	El Plan de Acción para Incidentes de Seguridad Informática debe incluir las siguientes fases y elementos esenciales:

A. PREPARACIÓN

- Designar y documentar los datos del responsable del plan.
- Crear un equipo especializado para atender incidentes de seguridad.
- Identificar e inventariar los procesos y activos de información.
- Clasificar los activos de información según su importancia.
- Elaborar una matriz de gestión de riesgos.
- Identificar posibles incidentes que puedan afectar la continuidad operativa.
- Definir la capacidad de almacenamiento del Ente.
- Establecer medidas de protección y respaldo de la información digital.
- Determinar los canales de comunicación para alertas de incidentes.

B. DETECCIÓN Y EVALUACIÓN

- Asignar roles y responsabilidades a cada área y personal involucrado.
- Implementar mecanismos para monitorear redes y sistemas en busca de actividades maliciosas.

Componentes:

- Detección
- Evaluación y clasificación de incidentes
- Tiempos de respuesta
- Notificación de incidentes

C. CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

- Implementar procedimientos de contención y erradicación de amenazas.
- Planificar estrategias de recuperación para restaurar la normalidad operativa.

D. ACTIVIDADES POST-INCIDENTE

- Revisar y fortalecer la gestión de riesgos en función de la experiencia adquirida.

	Recomendación: Integrar el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos del Gobierno Federal y el Marco de Seguridad Cibernética NIST (CSF) 2.0 del Instituto Nacional de Estándares y Tecnología de EE. UU. (2024).
DESCRIPCIÓN DEL REQUERIMIENTO:	El Instituto Tecnológico Superior de Cajeme deberá elaborar un Plan de Gestión de Incidentes de Seguridad Informática, adaptado a sus objetivos estratégicos y necesidades operativas. Este plan será enviado a la Subsecretaría de Gobierno Digital, a través de la Dirección General de Informática de la Secretaría de Educación y Cultura.
PRIORIDAD DEL REQUERIMIENTO:	Alta

3. ALCANCE

El Plan de Gestión de Incidentes de Seguridad Informática contiene las acciones de prevención y corrección de los incidentes que puedan originarse en los servicios esenciales del Instituto Tecnológico Superior de Cajeme.

4. REFERENCIAS

TITULO DEL DOCUMENTO	REFERENCIA
Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos	https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf
El Marco de Seguridad Cibernética (CSF) 2.0 del NIST	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf
ATT&CK Matrix for Enterprise	MITRE ATT&CK®

5. A. PREPARACIÓN

5.1. - I. El Plan deberá contener los datos generales de la persona servidora pública designada como responsable

RESPONSABLE DE EJECUCION DEL PLAN	
Nombre completo	Tadrio Eugenio Teran Serrano
Puesto que desempeña	Jefe Departamento de TIC
Correo institucional	tteran@itesca.edu.mx
Número de teléfono celular	+52-644-998-3924

5.2 - II. Equipo de atención de incidentes de seguridad

ROL	ADMINISTRADOR DE SEGURIDAD PERIMETRAL
Nombre completo	Ignacio Eduardo Urbalejo Rios
Puesto que desempeña	Encargado del área de redes y telecomunicaciones
Correo institucional	iurbalejo@itesca.edu.mx
Número de teléfono celular	+52-644-122-0313
Responsabilidades	Soporte técnico, administración, configuración y mantenimiento a los equipos de telecomunicaciones y a la infraestructura de la red cableada e inalámbrica.

ROL	ADMINISTRADOR CENTRO DE DATOS
Nombre completo	Norma Lilia Saucedo Ochoa
Puesto que desempeña	Responsable centro de datos
Correo institucional	lsaucedo@itesca.edu.mx
Número de teléfono celular	+52-644-200-6201
Responsabilidades	Administración, mantenimiento y configuración de servidores, administrador de dominio, realizar respaldos de todos los sistemas institucionales, administrador de cuentas de correo electrónico del personal docente, administrativo y de las cuentas de dominio.

ROL	ADMINISTRADOR DE INFRAESTRUCTURA
Nombre completo	Tadrio Eugenio Teran Serrano
Puesto que desempeña	Jefe Departamento de TIC
Correo institucional	tteran@itesca.edu.mx
Número de teléfono celular	+52-644-998-3924
Responsabilidades	Manejo del personal a cargo del área de tic, administración de infraestructura de sistemas y tecnológica de la institución para garantizar su correcta operación y funcionalidad.

ROL	ADMINISTRADOR DE SEGURIDAD DE CLIENTES (ANTIVIRUS)
Nombre completo	Manuel de Jesús Pórtela Enríquez
Puesto que desempeña	Encargado del área de taller de mantenimiento equipo de cómputo
Correo institucional	mportela@itesca.edu.mx
Número de teléfono celular	+52-644-196-4860
Responsabilidades	Mantenimiento correctivo preventivo a equipos de cómputo, instalación de software adicional office, antivirus etc..

ROL	ADMINISTRADOR DE MESA DE AYUDA
Nombre completo	Luis Daniel Rios Muñoz
Puesto que desempeña	Coordinador área de desarrollo de software
Correo institucional	drios@itesca.edu.mx
Número de teléfono celular	+52-644-100-5286
Responsabilidades	Mantenimiento, actualización y desarrollo de los sistemas instruccionales.

5.3 - Tabla de elevación de incidentes

Nivel de gravedad	Descripción	Acción requerida	Contacto inicial
Bajo	Impacto mínimo con interrupciones menores o sin interrupciones.	Monitorear el incidente, aplicar soluciones simples, sin necesidad de escalar.	Soporte Técnico o Equipo de Sistemas.
Medio	Interrupción parcial del servicio, afectando a usuarios no críticos.	Identificar la causa raíz, aplicar medidas correctivas y notificar al supervisor.	Supervisor del Área Técnica o Responsable de TIC.
Alto	Interrupción significativa del servicio, afectando a usuarios críticos.	Escalar al equipo de administración de TI, iniciar medidas correctivas urgentes.	Jefe de TIC o Gerente de Operaciones.
Crítico	Interrupción completa del servicio, afectando a todos los usuarios.	Activar el plan de contingencia, convocar a un comité de emergencia y escalar a la alta dirección.	Director de TIC, Alta Dirección o Comité de Crisis.

5.4 - Contacto Crítico

CONTACTO CRÍTICO	
Nombre completo	Tadrio Eugenio Teran Serrano
Puesto que desempeña	Jefe Departamento de TIC
Correo institucional	tteran@itesca.edu.mx
Número de teléfono celular	+52-644-998-3924

5.5 - III. Identificar e inventariar sus procesos y activos de información

Nombre del activo	Descripción del activo	Tipo de activo	Propietario del activo	Custodio del activo	Proceso al que está asociado	Ubicación física /digital	Nivel de clasificación de la información	Criticidad
Base de Datos	Información sobre alumnos, docentes y administrativos	Físico	Sistema Institucional	Luis Daniel Ríos Muñoz	Administrativo y operativo	Site Edificio 5	Alta	10
Contabilidad	Información contable de la institución	Físico	Sistema Institucional	Norma Lilia Saucedo Ochoa	Administrativo y contable	Site Edificio 5	Alta	10
Facturación	Información de facturas emitidas	Físico	Sistema Institucional	Norma Lilia Saucedo Ochoa	Administrativo y contable	Site Edificio 5	Alta	10
SACG	Información de sistemas contables	Físico	Sistema Institucional	Norma Lilia Saucedo Ochoa	Administrativo y contable	Site Edificio 5	Alta	10
Sitio	Información relacionada con las actividades de la institución	Físico	Sistema Institucional	Norma Lilia Saucedo Ochoa	Administrativo y operativo	Site Edificio 5	Alta	9

5.6 .- IV. Clasificar sus activos de información

Clasificar sus activos de información almacenada y procesada digitalmente				
Nombre del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Clasificación
Base de datos	☒CUMPLE	☒CUMPLE	☒CUMPLE	Alta
Contabilidad	☒CUMPLE	☒CUMPLE	☒CUMPLE	Alta
Facturación	☒CUMPLE	☒CUMPLE	☒CUMPLE	Alta
SACG	☒CUMPLE	☒CUMPLE	☒CUMPLE	Alta
Sitio	☒CUMPLE	☒CUMPLE	☒CUMPLE	Alta

Clasificar activos informáticos o infraestructura tecnológica				
Nombre del activo	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	Clasificación
Base de datos	☒CUMPLE	☒CUMPLE	☒CUMPLE	Alta
Contabilidad	☒CUMPLE	☒CUMPLE	☒CUMPLE	Alta
Facturación	☒CUMPLE	☒CUMPLE	☒CUMPLE	Alta
SACG	☒CUMPLE	☒CUMPLE	☒CUMPLE	Alta
Sitio	☒CUMPLE	☒CUMPLE	☒CUMPLE	Alta

ALTA	Aquellos activos en los cuales la información almacenada y procesada digitalmente cumple con dos o todas las propiedades de la información (confidencialidad, integridad, y disponibilidad).
MEDIA	Aquellos activos de información para los que la información almacenada y procesada digitalmente resulta alta en al menos una propiedad.
BAJA	Son los activos de información en los que su clasificación de información, para las tres propiedades se considera como baja.

5.7 . - V. Elaborar una matriz de gestión de riesgos

5.7.1 Impacto y Probabilidad de Ocurrencia

Impacto		
Valor que se asigna en una escala del 1 al 10, donde el de mayor jerarquía equivale a 10 y el de menor a 1.		
Escala de Valor	**Impacto**	**Descripción**
10	Catastrófico	Influye directamente en el cumplimiento de la misión, visión, metas y objetivos de la Institución y puede implicar pérdida patrimonial, incumplimientos normativos, problemas operativos o impacto ambiental y deterioro de la imagen, dejando además sin funcionar totalmente o por un periodo importante de tiempo, afectando los programas, proyectos, procesos o servicios sustantivos de la institución.
9		
8	Grave	Dañaría significativamente el patrimonio, incumplimientos normativos, problemas operativos o de impacto ambiental y deterioro de la imagen o logro de las metas y objetivos institucionales. Además, se requiere una cantidad importante de tiempo para investigar y corregir los daños.
7		
6	Moderado	Causaría, ya sea una pérdida importante en el patrimonio o un deterioro significativo en la imagen institucional.
5		
4	Bajo	Causa un daño en el patrimonio o imagen institucional, que se puede corregir en el corto tiempo y no afecta el cumplimiento de las metas y objetivos institucionales.
3		
2	Menor	Riesgo que puede ocasionar pequeños o nulos efectos en la institución.
1		

Probabilidad de ocurrencia		
Estimación de que se materialice un riesgo, en un periodo determinado.		
Escala de Valor	**Probabilidad de Ocurrencia**	**Descripción**
10	Recurrente	Probabilidad de ocurrencia muy alta. Se tiene la seguridad de que el riesgo se materialice, tiende a estar entre 90% y 100%
9		
8	Muy Probable	Probabilidad de ocurrencia alta. Está entre 75% a 89% la seguridad de que se materialice el riesgo
7		
6	Probable	Probabilidad de ocurrencia media. Está entre 51% a 74% la seguridad de que se materialice el riesgo
5		
4	Inusual	Probabilidad de ocurrencia baja. Está entre 25% a 50% la seguridad de que se materialice el riesgo
3		
2	Remota	Probabilidad de ocurrencia muy baja Está entre 1% a 24% la seguridad de que se materialice el riesgo
1		

5.7.2 Fichas de Riesgos Informático / VI. Identificar los diversos incidentes que podrían impactar la continuidad de las operaciones

5.7.2.1 R1 - IaaS (INFRAESTRUCTURA COMO SERVICIO – CENTRO DE DATOS)

Objetivos de Operación	**Mantener la operación segura del centro de datos de gobierno del estado, desde el cual diversos Entes y Dependencias proveen de servicios a la ciudadanía y las personas servidoras públicas.**
Clave - Activo	Site
Riesgo inherente	Sin servicio
Repercusiones	

Factores de riesgo externo

R #		Impacto (10-1)	Probabilidad de ocurrencia
E1	Desastres naturales	10	Remota
		9	
E2	Ciberataque y hacking	10	Inusual
		9	
E3	Falla eléctrica	10	Muy probable
		9	
E4	Vandalismo	8	Muy probable
		7	

Factores de riesgo interno

R #		Impacto	Probabilidad de ocurrencia
I1	Robo de información	8	Muy probable
		7	
I2	Virus	6	Probable
		5	
I3	Error humano	2	Remota
		1	
I4			

Respuesta a riesgos

Riesgos	Respuesta	Acciones
E1	Respaldos	Instalación de nueva infraestructura con la información recuperada de los respaldos
E2	Respaldos	Formatear y configurar los equipos afectados
E3	UPS	Revisar el tiempo de funcionamiento de la UPS y si la falla se va prolongar apagar los equipos de forma adecuada para que no presenten problemas.

	E4	Reportes	Revisar el nivel del vandalismo y buscar opciones para seguir operando, mientras se soluciona el problema.
	I1	Respaldos	Verificar que la información no haya sido modificada, comprándola con los respaldos
	I2	Antivirus	Revisar primero los equipos de cómputo con problemas y aislarlos de la red para que no se propague el virus, verificar que todos los equipos tengan instalado y actualizado el antivirus
	I3	Solucionar	Intentar solucionar el error y después solicitar capacitación, siempre y cuando la falla fue por falta de adiestramiento

METAS O ESTRATEGIAS DE PREVENCION DE RIESGOS

RIESGOS	ACCIÓN	PERIODICIDAD
R1. Falla eléctrica	Implementar **Sistemas de Alimentación Ininterrumpida (UPS)** y generadores de respaldo, además de revisiones periódicas.	Mensual
R2. Ciberataques y hacking	Instalar y actualizar **firewalls**, **Sistemas de Prevención de Intrusos (IPS)**, y realizar auditorías de seguridad.	Diario
R3. Desastres naturales	Asegurar redundancia en la infraestructura, realizar **respaldos en ubicaciones geográficamente distantes**.	Trimestral
R4. Vandalismo y acceso no autorizado	Implementar **sistemas de seguridad física** como cámaras de vigilancia, controles de acceso biométrico y personal de seguridad.	Trimestral
R5. Falla de hardware	Implementar políticas de **mantenimiento preventivo**, realizar pruebas periódicas de equipos críticos y tener un plan de reemplazo rápido.	Mensual
R6. Robo de información	Encriptar los datos en reposo y en tránsito, implementar **controles de acceso basados en roles** y monitoreo continuo de los sistemas.	Semestral
R7. Falla de sistema de refrigeración	Monitorear constantemente las condiciones ambientales del centro de datos e instalar sistemas de **refrigeración redundantes**.	Mensual
R8. Errores humanos	Capacitar regularmente al personal en **mejores prácticas de seguridad** y realizar simulacros de incidentes de seguridad.	Mensual

5.7.3 R2 - PaaS (PLATAFORMA COMO SERVICIO – CORREO ELECTRONICO/ANTIVIRUS)

Objetivos de Operación	**Mantener la operación y disponibilidad de las plataformas de administración de correo electrónico y antivirus que brindan servicio a las dependencias y personas servidoras públicas del Gobierno del Estado de Sonora.**
Clave - Activo	Servidor de Antivirus y correo
Riesgo inherente	Falla de servidor o falta de actualización de antivirus
Repercusiones	Sin servicio de correo y equipos con virus

Factores de riesgo externo

R #		Impacto (10-1)	Probabilidad de ocurrencia
E1	Sin servicio de internet por tiempo prolongado	8	Muy probable
		7	
E2	Falla eléctrica	8	Muy probable
		7	
E3	Falla de la plataforma de google workspace educativo	8	Remota
		7	
E4			

Factores de riesgo interno

R #		Impacto	Probabilidad de ocurrencia
I1	Renovación de licencia de antivirus	8	Probable
		7	
I2	Falla del servidor DNS	8	Inusual
		7	
I3	Falla del servidor de antivirus	8	Inusual
		7	
I4	Equipos de cómputo sin antivirus	8	Inusual
		7	

Respuesta a riesgos

Riesgos	Respuesta	Acciones
E1	Utilizar wifi	Reportar el incidente al proveedor de internet, si la falla se prolonga administrar antenas WIFI siempre y cuando el servicio WIFI no este afectado.
E2	UPS	Revisar con el área correspondiente si es problema de las instalaciones de la institución o falla de la CFE, para proceder a levantar el reporte correspondiente y el tiempo de solución, para verificar si el tiempo que le queda a la UPS Sistema de alimentación ininterrumpida es suficiente o se tienen que apagar los servidores.

E3	Utilizar otros medios de comunicación	Investigar la situación y el tiempo de respuesta, avisar a la comunidad institucional para que utilizan otros medios de comunicación
I1	Adquisición	Comunicarse con el proveedor del antivirus para adquirir la licencia
I2	Corrección	Revisar la falla del servidor DNS para corregirlo a la brevedad posible.
I3	Corrección	Revisar la falla del servidor antivirus y corregirla lo antes posible.
I4	Revisión	Instalar y/o actualizar los equipos de cómputo que no tienen instalado o actualizado el antivirus

METAS O ESTRATEGIAS DE PREVENCION DE RIESGOS

RIESGOS	ACCIÓN	PERIODICIDAD
R1. Falla del servidor de correo	Implementar **servidores redundantes** y configuraciones de **alta disponibilidad**, además de realizar pruebas periódicas de recuperación.	Mensual
R2. Sin servicio de internet	Contar con **proveedores de internet alternativos** y sistemas de **conmutación automática** en caso de fallo del proveedor principal.	Mensual
R3. Falta de actualización del antivirus	Automatizar las **actualizaciones del antivirus** en todos los dispositivos conectados a la red y monitorear los sistemas en tiempo real.	Semanal
R4. Ciberataques (phishing, malware)	Implementar **filtros avanzados de correo electrónico** para detectar phishing y malware, además de realizar simulaciones de ataques.	Diario
R5. Falla en la autenticación del correo	Habilitar **autenticación multifactor (MFA)** para acceder al sistema de correo y revisar logs de acceso para identificar intentos no autorizados.	Mensual
R6. Licencias de antivirus vencidas	Monitorear y renovar las **licencias del antivirus** de forma proactiva, con sistemas de alertas anticipadas.	Semestral
R7. Falla del servidor DNS	Configurar **servidores DNS redundantes** y monitorear su funcionamiento para garantizar la disponibilidad del servicio de correo.	Diario
R8. Equipos sin antivirus actualizado	Establecer **políticas de instalación forzada** para que todos los equipos conectados tengan el antivirus actualizado.	Semanal
R9. Acceso no autorizado al	Monitorear el acceso al servidor de correo y los logs, y configurar **alertas automáticas** para accesos sospechosos o no autorizados.	Diario

	servidor de correo		

5.8 Matriz de Riesgos

R1 - IaaS (INFRAESTRUCTURA COMO SERVICIO – CENTRO DE DATOS)

Probabilidad	Impacto									
	Catastrófico (10 / 9)		Grave (8 / 7)		Moderado (6 / 5)		Bajo (4 / 3)		Menor (2 / 1)	
Recurrente (10 / 9)	E	E	E	E	E	E	A	A	M	M
Muy probable (8 / 7)	E R1	E R2	E	E R7	A	A	M	M	B	B
Probable (6 / 5)	E	E R6	A R4	A R5	A R8	A	M	M	B	B
Inusual (4 / 3)	A R3	A	M	M	M	M	B	B	B	B
Remota (2 / 1)	M	M	B	B	B	B	B	B	B	B

Escalas de Colores			
B	Zona de Riesgo Baja	Asumir el Riesgo	
M	Zona de Riesgo Moderado	Asumir el Riesgo / Reducir el Riesgo	
A	Zona de Riesgo Alta	Reducir el Riesgo / Evitar / Transferir	
E	Zona de Riesgo Extrema	Reducir el Riesgo / Evitar / Compartir o Transferir	

R2 - PaaS (PLATAFORMA COMO SERVICIO – CORREO ELECTRONICO/ANTIVIRUS)

Probabilidad	Impacto									
	Catastrófico (10 / 9)		Grave (8 / 7)		Moderado (6 / 5)		Bajo (4 / 3)		Menor (2 / 1)	
Recurrente (10 / 9)	E	E	E	E	E	E	A	A	M	M
Muy probable (8 / 7)	E	E R3, R4	E	E	A	A	M	M	B	B
Probable (6 / 5)	E	E R9	A R1	A R2	A R8	A R7	M	M	B	B
Inusual (4 / 3)	A	A	M	M	M R5, R6	M	B	B	B	B
Remota (2 / 1)	M	M	B	B	B	B	B	B	B	B

Escalas de Colores		
B	Zona de Riesgo Baja	Asumir el Riesgo

M	Zona de Riesgo Moderado	Asumir el Riesgo / Reducir el Riesgo	
A	Zona de Riesgo Alta	Reducir el Riesgo / Evitar / Transferir	
E	Zona de Riesgo Extrema	Reducir el Riesgo / Evitar / Compartir o Transferir	

5.9 - VII. Definir la capacidad de almacenaje que tiene el Ente para su información

NOMBRE DEL ALMACENAMIENTO (NOMBRE DEL EQUIPO + CARDINALIDAD/CLASIFICACION)	TIPO DE TECNOLOGIA (HDD+RPM/SSD/NVME/SAS+RPM)	CAPACIDAD (USABLE)	UNIDAD
Base de Datos/Alta	Portable SSD /XS2000SSD	2 TB	1
Contabilidad/Alta	Portable SSD /XS2000SSD	1TB	1
Facturación/Alta	Portable SSD /XS2000SSD	1 TB	1
SACG/Alta	Portable SSD /XS2000SSD	1TB	1
Sitio/Alta	Portable SSD /XS2000SSD	1 TB	1

5.10 - VIII. Definir la protección y respaldo de la información almacenada y procesada digitalmente

Esquema de protección y respaldo de la información	SERVIDORES "INTERNOS" OFICIALIA MAYOR
Tipo de respaldo que realizan (incremental, parcial o total)	Parcial
Información que respaldan	Base de datos
Periodicidad con que lo hacen	Diario
Medios de respaldo que utilizan (unidad externa, Discos Duros de Estado Sólido o la nube)	Unidad externa
Medidas alternas de almacenamiento	DVD, Nube
Ubicación donde se encuentra almacenada la base datos de operación y la base de datos de respaldo.	Oficina Tic´s

Esquema de protección y respaldo de la información	SERVIDORES "INTERNOS" OFICIALIA MAYOR
Tipo de respaldo que realizan (incremental, parcial o total)	Parcial
Información que respaldan	Contabilidad
Periodicidad con que lo hacen	Diario

Medios de respaldo que utilizan (unidad externa, Discos Duros de Estado Sólido o la nube)	Unidad externa
Medidas alternas de almacenamiento	Disco Duro
Ubicación donde se encuentra almacenada la base datos de operación y la base de datos de respaldo.	Oficina Tic´s

Esquema de protección y respaldo de la información	**SERVIDORES "INTERNOS" OFICIALIA MAYOR**
Tipo de respaldo que realizan (incremental, parcial o total)	Parcial
Información que respaldan	Facturación
Periodicidad con que lo hacen	Diario
Medios de respaldo que utilizan (unidad externa, Discos Duros de Estado Sólido o la nube)	Unidad externa
Medidas alternas de almacenamiento	Disco Duro
Ubicación donde se encuentra almacenada la base datos de operación y la base de datos de respaldo.	Oficina Tic´s

Esquema de protección y respaldo de la información	**SERVIDORES "INTERNOS" OFICIALIA MAYOR**
Tipo de respaldo que realizan (incremental, parcial o total)	Parcial
Información que respaldan	SACG
Periodicidad con que lo hacen	Diario
Medios de respaldo que utilizan (unidad externa, Discos Duros de Estado Sólido o la nube)	Unidad externa
Medidas alternas de almacenamiento	Disco Duro
Ubicación donde se encuentra almacenada la base datos de operación y la base de datos de respaldo.	Oficina Tic´s

Esquema de protección y respaldo de la información	**SERVIDORES "INTERNOS" OFICIALIA MAYOR**
Tipo de respaldo que realizan (incremental, parcial o total)	Parcial
Información que respaldan	Sitio
Periodicidad con que lo hacen	Semanal
Medios de respaldo que utilizan (unidad externa, Discos Duros de Estado Sólido o la nube)	Unidad externa
Medidas alternas de almacenamiento	Nube
Ubicación donde se encuentra almacenada la base datos de operación y la base de datos de respaldo.	Oficina Tic´s

EJEMPLO DE RESULTADO DE TRABAJO DE RESPALDO INTERNO					
Fecha	**Tipo de Respaldo**	**Descripción del Activo Respaldado**	**Medio de Almacenamiento**	**Ubicación del Respaldo**	**Observaciones**
21/10/2024	Incremental	Base de datos del sistema de nómina	Unidad de Almacenamiento Inteno (SSD)	Servidor interno - Rack 3	Verificación exitosa, sin errores.
14/10/2024	Completo	Sistema de gestión documental	Discos duros internos RAID	Almacenado en servidor interno principal	Copia completa. Integridad validada.
07/10/2024	Incremental	Aplicaciones de usuarios (Directorio Activo)	Servidor de almacenamiento	Servidor de respaldo interno - Site A	Respaldado y verificado correctamente.
30/09/2024	Completo	Información de la intranet institucional	Discos SSD internos	Servidor dedicado de respaldo - Área técnica	Completado sin incidencias.

EJEMPLO DE RESULTADO DE TRABAJO DE RESPALDO EXTERNO					
Fecha	**Tipo de Respaldo**	**Descripción del Activo Respaldado**	**Medio de Almacenamiento**	**Ubicación del Respaldo**	**Observaciones**
22/10/2024	Incremental	Base de datos del sistema de gestión académica	Unidad de Almacenamiento Externo (SSD)	Almacenado en Data Center Externo – Site B	Verificado. Sin errores
15/10/2024	Completo	Información de correo electrónico institucional	Nube Privada	Almacenado en servidor cloud de proveedor externo	Completo. Validación exitosa del respaldo.
08/10/2024	Incremental	Sistema de virtualización del servidor principal	Discos Duros Externos	Data Center Externo – Site C	Verificación en curso.
01/10/2024	Completo	Información administrativa de recursos humanos	Nube Privada	Backup en servidor cloud (AWS)	Respaldado correctamente.

5.11 - IX. Establecer los canales de comunicación

A continuación, se definen para la Oficialía Mayor los canales de comunicación a través de los cuales se podrá comunicar cualquier alerta que implique la ocurrencia de un incidente.

a. Enviando un mensaje de correo electrónico tteran@itesca.edu.mx, comitetics@itesca.edu.mx

b. Llamando al teléfono (644)410-8671

6. - B. DETECCIÓN Y EVALUACIÓN

En esta etapa, se debe establecer en el Plan para la Gestión de Incidentes de Seguridad Informática, los roles y responsabilidades del ejecutor, de las demás áreas y del personal que integran al Ente, a fin de que el personal designado para la atención y gestión de elementos que alertan sobre un incidente pueda estar preparados con procedimientos previamente establecidos para minimizar su impacto.

6.1 - Los roles y responsabilidades del ejecutor

Responsabilidades que aseguran una respuesta estructurada y efectiva a los incidentes de seguridad informática, minimizando la interrupción del negocio, la pérdida de datos y el daño reputacional:

1. Preparación: Asegurar que el equipo esté preparado para responder a incidentes de seguridad. Esto incluye la capacitación del personal y la implementación de herramientas y procesos necesarios.
2. Comunicación y coordinación: Mantener una comunicación clara y efectiva con todos los miembros del equipo y las partes interesadas. Esto incluye la notificación de incidentes al Subsecretario de Gobierno Digital y sus Direcciones Generales, así como a las dependencias y entidades de la administración pública estatal.
3. Escalamiento: Escalar el incidente con los proveedores, a los equipos legales o a las autoridades cuando sea necesario.
4. Contención, erradicación y recuperación: Implementar medidas para contener el incidente, eliminar la amenaza y restaurar los sistemas afectados a su estado normal. Esto puede incluir la desconexión de sistemas comprometidos, la eliminación de *malware* y la restauración de datos desde copias de seguridad.
5. Documentación y reporte: Documentar todas las acciones tomadas durante la respuesta al incidente y preparar informes detallados para su análisis posterior. Esto ayuda a identificar áreas de mejora y a prevenir futuros incidentes.
6. Mejora continua: Evaluar la efectividad de la respuesta al incidente y realizar mejoras continuas en el plan de gestión de incidentes. Esto incluye la revisión de políticas y procedimientos, la actualización de herramientas y la capacitación continua del personal.

Tareas del responsable de ejecución del plan:

1. Activar el plan de respuesta de acuerdo con los procedimientos establecidos.
2. Asignar tareas específicas a cada miembro del equipo.
3. Monitorear el progreso de la investigación y resolución.
4. Asegurar que se cumplan los objetivos del plan de respuesta.
5. Escalar el incidente de acuerdo con lo reportado por el equipo.
6. Alineación con el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos y el NIST.

6.2 De las demás áreas y del personal que integran al Ente

6.2.1 Administrador de seguridad perimetral

1. Monitoreo y análisis: Supervisar y analizar los eventos de seguridad relacionados con el firewall para identificar posibles incidentes. Esto implica revisar los registros del firewall y utilizar herramientas de monitoreo para detectar actividades sospechosas.
2. Implementación de medidas de contención: Colaborar con el administrador del centro de datos y otros miembros del equipo para implementar medidas de contención durante un incidente. Esto puede incluir la actualización de reglas del firewall para bloquear tráfico malicioso y la segmentación de la red para limitar la propagación del incidente.
3. Actualización de configuraciones: Asegurar que las configuraciones del firewall estén actualizadas y sean efectivas para proteger contra amenazas conocidas. Esto incluye la aplicación de actualización de las definiciones de los módulos de seguridad.
4. Comunicación y coordinación: Mantener una comunicación clara y efectiva con todos los miembros del equipo y las partes interesadas. Esto incluye la notificación de incidentes a el responsable de ejecución del plan y otras dependencias.
5. Documentación y reporte: Documentar todas las acciones tomadas durante la respuesta al incidente y preparar informes detallados para su análisis posterior. Esto ayuda a identificar áreas de mejora y a prevenir futuros incidentes.
6. Mejora continua: Evaluar la efectividad de las medidas de seguridad del firewall y realizar mejoras basadas en las lecciones aprendidas durante el incidente.

Después del Incidente:

1. Análisis post-incidente: Participar en el análisis *post-mortem* para identificar las causas raíz del incidente y las deficiencias en los procesos de seguridad.
2. Actualización de políticas y procedimientos: Revisar y actualizar las políticas y procedimientos de seguridad para abordar las vulnerabilidades expuestas durante el incidente.
3. Capacitación: Capacitar al personal sobre las lecciones aprendidas del incidente y mejorar su conciencia sobre las amenazas cibernéticas.

Tareas del administrador del firewall

1. Monitoreo: Analizar el estado de la implementación del firewall en búsqueda de patrones y tendencias que puedan indicar una amenaza, desde variaciones del performance, estado de la memoria o número de conexiones atípicas.
2. Supervisión de Logs: Analizar los logs del firewall para detectar cualquier actividad sospechosa o intentos de intrusión.
3. Identificación de reglas: Identificar y responder a los intentos de intrusión en la red.
4. Identificación de sistemas comprometidos: Mediante el uso de las herramientas analíticas.
5. Aislamientos de sistemas: Aislar los sistemas comprometidos para evitar la propagación en la red, bloqueando sus comunicaciones.
6. Modificación de reglas: Realizando los ajustes que aseguren la contención y robustecimiento de la red y centro de datos.
7. Comunicación y coordinación: Mantener una comunicación clara y efectiva con todos los miembros del equipo y las partes interesadas. Esto incluye la notificación de incidentes al ejecutor del plan y la coordinación con otras dependencias y/o proveedores si es necesario.
8. Creación de reportes y documentación: Documentar todas las acciones tomadas durante la respuesta al incidente y preparar informes detallados para su análisis posterior.
9. Diseñar y ejecutar: Políticas, actualizaciones y configuraciones del firewall.

6.2.2 Administrador de centro de datos

1. Monitoreo y mantenimiento: Supervisar y mantener las condiciones físicas de los servidores y otros componentes de la infraestructura de TI.
2. Gestión de sistemas críticos: Monitorear los sistemas de enfriamiento, energía y otros sistemas críticos de los que depende el centro de datos.
3. Soporte de control de acceso: Apoyar los sistemas de control de acceso que protegen contra riesgos de seguridad física.
4. Implementación de medidas de contención: Colaborar con el administrador de firewall y otros miembros del equipo para implementar medidas de contención durante un incidente. Esto puede incluir la desconexión de sistemas comprometidos.

5. Administración y ejecución de respaldos: Crear, administrar y ejecutar respaldos en el centro de datos, garantizando la integridad y disponibilidad de datos en caso de fallas.
6. Restauración de sistemas: Trabajar en la recuperación y restauración de los sistemas afectados a su estado normal. Esto puede incluir la restauración de datos desde copias de seguridad y la verificación de que los sistemas están funcionando correctamente.
7. Comunicación y coordinación: Mantener una comunicación clara y efectiva con todos los miembros del equipo y las partes interesadas. Esto incluye la notificación de incidentes al ejecutor del plan y la coordinación con otras dependencias y/o proveedores si es necesario.
8. Documentación y reporte: Documentar todas las acciones tomadas durante la respuesta al incidente y preparar informes detallados para su análisis posterior.

Tareas de administración de centro de datos:

1. Detección y notificación del incidente en coordinación con el área de seguridad perimetral para proceder a informar al responsable de ejecución del plan.
2. Determinar que sistemas, servidores o activos de información se encuentran comprometidos, mediante el análisis del performance del servidor de virtualización y servidor virtual.
3. Analizar el nivel de afectación procurando el aislamiento del incidente en sus diferentes capas:
    a. Nivel servidor virtual
    b. Nivel de virtualización
    c. Nivel servidor físico
    d. Nivel grupo de servidores físicos
    e. Nivel sistema de respaldos
    f. Nivel sitio

4. Ejecutar el aislamiento para protección de contaminación lateral, aislamiento total de sitio o inclusive apagado de equipo en sitio para dar pie a la activación de sitio alterno para la continuidad de los servicios por medio del sistema *failover* en imágenes de replicación.
5. Mantener en todo momento la comunicación con el ejecutor del plan de gestión enviando actualizaciones frecuentes sobre el estado del incidente, describiendo lo que se ha hecho, qué pasos siguen y los tiempos estimados para la resolución.
6. Buscar activamente la forma de implementar soluciones temporales para la restauración parcial de los servicios de la forma más eficiente posible.
7. Llevar a cabo la restauración de los sistemas afectados a su estado normal de operación. Restaurando los bloqueos para el restablecimiento de la operatividad de manera ordenada y siguiendo un programa de cambio de contraseñas para blindar los servicios restablecidos.
8. Asegurar que se cumplan las normativas de seguridad aplicables al centro de datos.
9. Documentar el incidente para registrar los detalles, acciones y los resultados de estas a través de un informe que sirva como referencia futura.

6.2.3 Administrador de infraestructura

1. Análisis de la red: Monitorear la actividad de la red en busca de anomalías o tráfico sospechoso, identificando los puntos de entrada utilizados por el atacante.
2. Aislamiento del incidente: Identificar y aislar los sistemas o redes comprometidos para limitar la propagación del incidente.
3. Restaurar: Servicios y sistemas a un estado a un estado seguro y operativo.
4. Preservación de la evidencia: Capturar y preservar la evidencia digital de forma forense para futuras investigaciones y análisis.
5. Documentar: Mantener actualizada la documentación técnica de la infraestructura para facilitar la respuesta a futuros incidentes, así como los pasos realizados durante la gestión del incidente.
6. Coordinación con otros equipos: Colaborar estrechamente con el equipo de respuesta a incidentes, proporcionando información técnica detallada sobre la infraestructura afectada.

Tareas del administrador de infraestructura

1. Monitorear la actividad de la red mediante el uso de herramientas disponibles a fin de evidenciar la actividad por amenaza, y los logs de sistemas, aplicaciones y seguridad para identificar patrones de ataque y determinar la extensión de los servicios y sistemas comprometidos.
2. Identificar los puntos de entrada utilizados por el atacante y que se estén explotando.
3. Desconectar o interrumpir servicios y comunicaciones para contener la afectación del incidente y deshabilitar servicios innecesarios según sea requerido.
4. Aplicar parches de seguridad y/o bloqueos a los sistemas vulnerables, cambiando contraseñas de cuentas comprometidas.
5. Verificar la integridad de los servicios operativos restaurando los afectados
6. Validar la funcionalidad de los servicios y sistemas restaurados.
7. Realizar pruebas de penetración para identificar vulnerabilidades residuales.
8. Evaluar la efectividad de las medidas de seguridad implementadas.
9. Creación de reportes y documentación: Documentar todas las acciones tomadas durante la respuesta al incidente y preparar informes detallados para su análisis posterior.

6.2.4 Administrador del antivirus

1. Identificar y clasificar vulnerabilidades en los sistemas.
2. Identificar parches de seguridad de manera oportuna.
3. Realizar auditorías en la consola de antivirus para identificar posibles riesgos.
4. Desarrollar y ejecutar programas de capacitación para los empleados sobre seguridad informática.
5. Promover buenas prácticas de seguridad entre los usuarios.

6. Realizar investigaciones forenses para determinar la causa raíz de los incidentes.
7. Asegurar el cumplimiento de las normativas de seguridad de la información aplicables.
8. Identificar, evaluar y mitigar los riesgos de seguridad desde la perspectiva del antivirus

Tareas del administrador del antivirus

1. Selección de la solución: Evaluar y seleccionar la solución antivirus más adecuada para las necesidades de la organización, considerando factores como el tamaño de la red, el tipo de dispositivos y el presupuesto.
2. Instalación: Instalar y configurar el software antivirus en todos los sistemas de la dependencia, asegurando una cobertura completa.
3. Actualización: Mantener las definiciones de virus y las firmas de *malware* actualizadas en todos los sistemas.
4. Configuración de políticas: Establecer políticas de detección, limpieza y notificación para garantizar un nivel óptimo de protección.
5. Monitoreo de alertas: Supervisar de forma proactiva las alertas generadas por el sistema antivirus y analizarlas para determinar si representan una amenaza real.
6. Investigación de incidentes: Investigar a fondo las detecciones de *malware* para determinar la naturaleza de la amenaza y su alcance.
7. Eliminación de amenazas: Eliminar de forma segura el *malware* de los sistemas infectados y si es posible, restaurar los archivos dañados.
8. Contención: Implementar medidas para contener la propagación del *malware*, como aislar sistemas infectados.
9. Creación de informes: Generar informes periódicos sobre el estado de la seguridad de la dependencia y las amenazas detectadas.
10. Creación de reportes y documentación: Documentar todas las acciones tomadas durante la respuesta al incidente y preparar informes detallados para su análisis posterior.
11. Optimización del rendimiento: Optimizar la configuración del antivirus para minimizar el impacto en el rendimiento del sistema.
12. Gestión de excepciones: Gestionar las excepciones de forma cuidadosa para evitar falsos positivos y garantizar la protección del sistema.
13. Capacitación de usuarios: Capacitar a los usuarios sobre las mejores prácticas de seguridad para prevenir infecciones por *malware*.

6.2.5 Administrador de mesa de ayuda

1. Primer punto de contacto para recibir reportes de usuarios sobre actividades sospechosas, interrupciones del servicio o cualquier anomalía para su seguimiento.
2. Documentar de manera detallada cada reporte, incluyendo fecha, hora, usuario que reportó, descripción del incidente y cualquier otra información relevante que sea de ayuda para la atención del incidente.

3. Mantener informados a los usuarios sobre el estado de sus reportes y las acciones que se están tomando.
4. Proporcionar instrucciones claras y concisas a los usuarios para minimizar el impacto del incidente.
5. Actualizar la base de conocimientos con información sobre incidentes comunes y soluciones para mejorar la eficiencia en la resolución de futuros problemas.

Tareas del administrador de mesa de ayuda

1. Recibir el reporte para seguimiento, conformando la información necesaria realizando preguntas específicas al reportante para obtener más detalles sobre el incidente, como mensajes de error, acciones realizadas antes del incidente y cualquier otra información relevante.
2. Comunicar al responsable de la ejecución del plan para coordinación y seguimiento de la atención del incidente.
3. Realizar diagnósticos básicos, como verificar la conectividad de red, reiniciar equipos o verificar el estado de los servicios.
4. Aplicar medidas de control temporales, como bloquear el acceso a cuentas o recursos, mientras se espera la resolución definitiva del incidente.
5. Comunicar claramente a los usuarios los tiempos estimados de resolución y mantenerlos actualizados sobre el progreso de las acciones tomadas.
6. Dar seguimiento a los incidentes hasta su resolución completa y documentar las acciones realizadas y los resultados obtenidos.
7. Participación en la revisión post incidente: Contribuir con su perspectiva y conocimientos a la revisión post incidente para identificar áreas de mejora en los procesos y procedimientos.

6.3 MECANISMOS IMPLEMENTADOS DE MONITOREO DE RED Y DE SISTEMAS

De igual manera, se deben establecer los mecanismos para monitorear la red y sistemas en busca de señales de actividad maliciosa.

MECANISMOS IMPLEMENTADOS DE MONITOREO DE RED Y DE SISTEMAS	
OBJETIVO	**MECANISMO**
Detección de accesos no autorizados o actividad sospechosa	Uso de **Sistemas de Detección de Intrusos (IDS)** y **Sistemas de Prevención de Intrusos (IPS)**.
Monitoreo del tráfico de red en tiempo real	Implementación de herramientas como **Wireshark**, **NetFlow**, o **Snort** para analizar el tráfico de red.

Prevención de amenazas y malware	Uso de **Antivirus** y **software de protección contra malware** actualizados, incluyendo análisis programados.
Supervisión del estado de los servidores y dispositivos	Monitoreo mediante **sistemas de gestión de logs** como **SIEM (Security Information and Event Management)**.
Detección de vulnerabilidades en aplicaciones	Ejecución periódica de **escáneres de vulnerabilidades** como **Nessus** o **OpenVAS.**
Control de acceso y autenticación	Implementación de **sistemas de autenticación multifactor (MFA)** y **monitoreo de accesos** a través de logs.
Identificación de comportamientos anómalos en el uso de la red	Análisis de comportamiento del tráfico con herramientas como **User Behavior Analytics (UBA)** o **AI-driven SIEM**.
Gestión y actualización de configuraciones de seguridad	Uso de **herramientas de gestión de parches** y **auditorías periódicas de seguridad** para asegurar sistemas actualizados.
Detección de intentos de phishing y spam	Implementación de **filtros de correo electrónico avanzados** y análisis de contenido sospechoso en mensajes entrantes.
Supervisión de cambios no autorizados en los sistemas	Uso de herramientas de **monitoreo de integridad de archivos (FIM)** para detectar modificaciones no autorizadas.

6.4 - 1. Detección.

Los indicadores que a continuación se señalan de manera enunciativa más no limitativa, consisten en eventos que indican la posible ocurrencia de un incidente:

• Alertas en sistemas de seguridad.

• Caídas de servidores.

• Reportes de usuarios.

• Software antivirus dando informes.

• Otras anomalías fuera de lo normal del sistema.

Por ello se deberá utilizar el formato propuesto de registro de incidente con la finalidad de contar con la información base que sirva de guía o punto inicial en el trazo de la criticidad y problema al que el equipo se enfrenta.

Es importante establecer la información que debe integrar el servidor público que identifique el posible incidente, ya que generalmente esa información es utilizada para la atención del incidente y entre más documentado se encuentra éste existen más probabilidades de que sea atendido de manera exitosa con impactos mínimos.

Generalmente los incidentes se documentan con capturas de pantalla, correos electrónicos, fotografías, videos, entre otros.

Es importante llevar una bitácora sobre los incidentes reportados a efecto de reconocer patrones de comportamiento sospechoso.

6.5 - 2. Evaluación.

Ante cualquier alerta de un incidente o anomalía detectada, el ejecutor del Plan para la Gestión de Incidentes de Seguridad Informática inicia la investigación técnica para determinar la naturaleza del incidente, es decir, si se trata de un incidente de los que a continuación se señalan de manera enunciativa más no limitativa:

- De seguridad de la información
- Ciberataque
- De conectividad
- Falla eléctrica
- De infraestructura

Realiza una serie de preguntas a la persona que reporta el incidente y reúne cualquier tipo de evidencia que permita analizar el código dañino.

Una vez clasificado el incidente de seguridad, realiza una evaluación para categorizar su impacto, con base en la matriz de riesgos y la clasificación de activos de información que previamente se han establecido en dicho Plan.

Los Entes deben clasificar sus incidentes con base en los siguientes criterios de severidad:

a. Alto impacto: El incidente de seguridad afecta a activos de información considerados de criticidad alta, tienen efectos catastróficos, ya que influyen directamente en los servicios esenciales del Ente. Estos incidentes deben tener respuesta inmediata.

b. Medio impacto: El incidente de seguridad afecta a activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado.

c. Bajo impacto: El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

6.6 - 3. Clasificación de incidentes

Una vez evaluado el incidente, se debe clasificar su nivel de criticidad, utilizando el siguiente criterio:

Nivel de Criticidad
Crítico
Muy Alto
Alto
Medio
Bajo

6.7 - 4. Tiempos de Respuesta

Para el caso de la atención de incidentes de seguridad se han establecido unos tiempos máximos de atención de éstos, con el fin de atender adecuadamente los incidentes de acuerdo con su criticidad e impacto. Los tiempos expresados en la siguiente tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido.

Nivel de Criticidad	Tiempo de respuesta
Crítico	2 horas
Muy Alto	1 hora
Alto	30 minutos
Medio	15 minutos
Bajo	5 minutos

Cabe resaltar que cada Ente debe definir sus tiempos de respuesta a incidentes dependiendo de la criticidad de los activos impactados.

6.8 - 5. Notificación de Incidentes

Ante la sospecha sobre la materialización de un incidente de seguridad, el servidor público que lo detecte deberá notificar de inmediato a la persona servidora pública responsable de la ejecución del Plan para la Gestión de Incidentes de Seguridad Informática, a través de cualquier canal de comunicación.

Para la formalización de la notificación de incidencias, se debe establecer un formato, en el cual el usuario que reporta el incidente debe diligenciar con la mayor cantidad posible de información relacionada con el incidente.

El ejecutor del Plan para la Gestión de Incidentes de Seguridad Informática será el encargado de realizar el seguimiento del Incidente hasta su cierre definitivo.

De haber acciones inmediatas, se brindan consejos iniciales y de existir, se proporcionará la información sobre procedimientos aplicables para el incidente en particular para su resolución.

Se documentan las alternativas de solución de acuerdo con la criticidad de los activos de información y se llevan a cabo reuniones de trabajo para identificar la viabilidad de su aplicación.

La persona encargada de la atención de incidentes tendrá la atribución para decidir sobre las acciones que se deban ejecutar ante la presencia de un incidente de seguridad informática, siempre salvaguardando la integridad y totalidad de la información que se encuentra en riesgo. Si es necesario, el Ente deberá emitir un comunicado a la ciudadanía o sector afectado, con el objeto de comunicar la situación y se tomen las medidas pertinentes para minimizar las afectaciones a la prestación de trámites y servicios gubernamentales.

Cuando se identifiquen incidentes cibernéticos clasificados como "Críticos", "Muy Altos" o "Altos" y ha concluido el tiempo de respuesta establecido en su Plan para la Gestión de Incidentes de Seguridad Informática y no se ha logrado reactivar las operaciones esenciales del Ente, el incidente deberá ser considerado como una situación de emergencia, por lo que realizará de manera inmediata la notificación a la Subsecretaría a través de los siguientes canales:

a. Enviando un mensaje de correo electrónico a mesadeayuda@sonora.gob.mx

b. Llamando al teléfono (662) 319 3796 ext. 1022.

7. - C. CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

La contención busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TIC, para facilitar esta tarea los Entes deben poseer una estrategia de contención previamente definida para poder tomar decisiones.

En el proceso de contención, los Entes deben dar prioridad al cumplimiento de tres acciones:

1. Aislamiento: Esto implica la separación de los sistemas comprometidos para evitar la propagación.

2. Bloqueo: Se debe impedir que el incidente cibernético se propague a otros dispositivos.

3. Desconexión: Es de suma importancia desconectar los sistemas afectados de la red.

Después de que el incidente ha sido contenido se debe realizar una erradicación, es decir, la eliminación de cualquier rastro dejado por el incidente de los sistemas afectados. Posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados, para lo cual el responsable de la ejecución del Plan debe restablecer la funcionalidad de los sistemas afectados con copias de seguridad limpias y realizar las modificaciones necesarias al sistema que permita prevenir incidentes similares en el futuro.

Una vez restaurados los sistemas se debe validar su integridad y comunicar a las demás partes interesadas sobre el incidente.

La Subsecretaría proveerá acompañamiento a los Entes en esta etapa ante incidentes cibernéticos clasificados como "Críticos", "Muy Altos" o "Altos".

8. - D. ACTIVIDADES POST-INCIDENTE

Las actividades Post-Incidente básicamente se componen del reporte apropiado del Incidente, de la generación de lecciones aprendidas y el establecimiento de medidas tecnológicas, disciplinarias y penales de ser necesarias.

Por último, se proporciona información no clasificada del incidente y el mecanismo utilizado a otros involucrados para ayudar a mejorar la seguridad de su infraestructura.

Mantener un adecuado registro de lecciones aprendidas a efecto de:

- Conocer exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Saber si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
- Conocer qué se debería hacer la próxima vez que ocurra un incidente similar.

• Conocer acciones correctivas pueden prevenir incidentes similares en el futuro.

• Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes.

• Actualizar políticas y procedimientos de seguridad, para prevenir incidentes similares en el futuro.

DÉCIMA SEGUNDA. Con la finalidad de nutrir la gestión de riesgos de seguridad cibernética se recomienda utilizar el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos del Gobierno Federal y consultar a manera de referencia el Marco de Seguridad Cibernética del NIST (CSF) 2.0 «Instituto Nacional de Estándares y Tecnología de los Estados Unidos de América (2024).

La Subsecretaría elaborará un Plan para la Gestión de Incidentes de Seguridad Informática, considerando al menos los pasos antes mencionados, en caso de que se ajuste a las necesidades y particularidades de la información de los Entes, éstos podrán adoptar y ajustar dicho Plan con los requerimientos que establece el presente instrumento, incluyendo el envío a la Subsecretaría.

9. Formato de Notificación de Incidente

FECHA Y HORA DE DETECCIÓN				**FECHA Y HORA DE REPORTE**			
MEDIO DE REPORTE	TELÉFONO	☐	CORREO	☐	CELULAR	☐	MESA DE AYUDA	☐
EVIDENCIA PRESENTADA	CAPTURA	☐	ARCHIVOS	☐	FOTOS	☐	VIDEO	☐

TIPO DE INCIDENTE (1)					
SERVIDOR NO RESPONSIVO	☐	FALLA ACCESO A CUENTA	☐	DEGRADACIÓN DE LA RED	☐
SERVIDOR SIN ESPACIO	☐	CONTRASEÑA	☐	FALLA EN TELEFONÍA	☐
SUBDOMINIO NO ACCESIBLE	☐	*MALWARE*	☐	BAJO RENDIMIENTO DE SISTEMA	☐
VPN CON FALLA	☐	PHISHING	☐	BAJO RENDIMIENTO DE APP	☐
SITIO CON FALLA	☐	SPAM	☐	PÉRDIDA DE DATOS	☐
ERROR DE CARGA	☐	ACCESO NO AUTORIZADO	☐	FALLA DE ACCESO A RECURSO	☐
OTRO	☐				

INFORMACIÓN DEL REPORTE (1)			
DESCRIPCIÓN DEL INCIDENTE			
SISTEMAS AFECTADOS		DATOS AFECTADOS	
IMPACTO EN LA OPERACIÓN		CRITICIDAD (MATRIZ RIESGO)	

ACCIONES TOMADAS	

INFORMACIÓN DEL REPORTANTE		INFORMACIÓN DE LA DEPENDENCIA	
NOMBRE		SECRETARÍA	
CELULAR		DEPENDENCIA	
CORREO		UNIDAD ADMINISTRATIVA	
UTIC			

ACCIONES INICIALES – DEFINICIÓN - EVALUACIÓN (2)									
RIESGO DE LATELARIDAD ☐		**RIESGO DE RANSOMWARE ☐**			**INFRAESTRUCTURA ☐**				
SEGURIDAD ☐	**CIBERATAQUE ☐**		**CONECTIVIDAD ☐**		**FALLA ELÉCTRICA ☐**		**VIRUS ☐**		
ESTATUS POR AREA:	FIREWALL		CENTRO DE DATOS		INFRAESTRUCTURA		ANTIVIRUS		
ASIGNACIÓN DE SEGUIMIENTO				HORA DE INICIO DE SEGUIMIENTO POR ÁREA DESIGNADA					
DIAGNÓSTICO INICIAL									
Nivel de Criticidad (3) - Tiempo de respuesta (4)									
☐ Crítico / 5 minutos		**☐ Muy Alto / 15 minutos**			**☐ Alto / 30 minutos**				
☐ Medio / 1 hora		**☐ Bajo / 2 horas**							

10. Formato de Seguimiento de Incidente

NOTIFICACIÓN DE INCIDENTES			
ACTIVIDADES APROPIADAS PARA TOMAR ACCION EN RELACIÓN CON UN EVENTO DE CIBERSEGURIDAD DETECTADO			
ÁREA		PERSONAL ASIGNADO	
ACCIONES			
IDENTIFICACIÓN https://attack.mitre.org/			
MONITOREO			
ANÁLISIS			
CONTENCIÓN AISLAMIENTO BLOQUEO DESCONEXIÓN			
ERRADICACIÓN			
RECUPERACIÓN			
HORA Y FECHA DE RETORNO DE OPERACIÓN			
REMEDIACIÓN			
RECOMENDACIONES			

Ing. Xxxx Xxxx Xxxxx	Ing. Xxxxx Xxxxxx Xxxxxx
DIRECTOR GENERAL	INGENIERO A CARGO

11. Anexo 1 – inventarios generales de equipamiento y conectividad

ENLACES DE CONECTIVIDAD				
TIPO DE ENLACE	**COMPAÑÍA**	**VELOCIDAD DE BAJADA (Mbps)**	**VELOCIDAD DE SUBIDA (Mbps)**	**NUMERO DE CONTRATO/ TELEFONO**
DEDICADO	TELMEX	200	200	3F35069 / 644108650
FTTH	TELMEX	1000	1000	0Q42260 / 6444108650
FTTH	TELMEX	1000	1000	0Q42260 / 6444108650
FTTH	TELMEX	1000	1000	0Q42260 / 6444108650
FTTH	TELMEX	1000	1000	0Q42260 / 6444108650
FTTH	TELMEX	1000	1000	0Q42260 / 6444108650

ENLACES DE TELEFONIA				
TIPO DE ENLACE	**COMPAÑÍA**	**LINEAS (TIPO)**	**DIDs (SI APLICA)**	**NUMERO DE CONTRATO/ TELEFONO**
TRONCAL IP	TELMEX	30 TRONCALES IP	100	0Q42260 / 6444108650

SEGURIDAD PERIMETRAL				
EQUIPO/SERIE	**MARCA**	**FECHA DE ADQUISICION**	**TIPO DE LICENCIAMIENTO**	**WAN EN USO**
FORTIGATE / FG100FTK23000114	FORTINET	28/10/2023	***STATUS*** VIGENTE ☐x	WAN 1 ☒ WAN 2 ☐ DMZ ☐

INFRAESTRUCTURA DE CONECTIVIDAD				
EQUIPO/SERIE	**MARCA**	**FECHA DE ADQUISICION**	**TIPO DE LICENCIAMIENTO**	**UBICACIÓN EN RACK**
SWITCH USW Pro 48 PoE / 784558baffb8	UBIQUITI	27/06/2022	PERMANENTE	RACK EDIFICIO 1
SWITCH SG200-50P / DNI213704J0	CISCO	15/05/2018	PERMANENTE	RACK EDIFICIO 2

SWITCH USW Pro 48 PoE / 784558e75c9e	UBIQUITI	27/06/2022	PERMANENTE	RACK EDIFICIO 3
SWITCH USW Pro 48 PoE / 784558e734ab	UBIQUITI	27/06/2022	PERMANENTE	RACK EDIFICIO 4
SWITCH USW Pro 48 PoE / 784558bad70b	UBIQUITI	27/06/2022	PERMANENTE	RACK EDIFICIO 5
SWITCH USW Pro 48 PoE / 784558bafc9d	UBIQUITI	27/06/2022	PERMANENTE	RACK EDIFICIO 6
SWITCH SF200-24P / DNI181503NV	CISCO	15/05/2018	PERMANENTE	RACK EDIFICIO 7
SWITCH USW Pro 48 PoE / 60223251bb24	UBIQUITI	27/06/2022	PERMANENTE	RACK EDIFICIO 8

INFRAESTRUCTURA EN SITE PRINCIPAL				
EQUIPO/SERIE	**MARCA**	**FECHA DE ADQUISICION**	**TIPO DE LICENCIAMIENTO**	**UBICACIÓN EN RACK**
SWITCH CORE / SG72G491B8	HP ARUBA	29/05/2017	PERMANENTE	RACK 3 EDIF 5
FIREWALL FORTIGATE / FG100FTK23000114	FORTINET	28/10/2023	ANUAL	RACK 4 EDIF 5
CONMUTADOR IP OFFICE 500 V2 / 19WZ5020C01P	AVAYA	11/09/2020	ANUAL (3 AÑOS)	RACK 3 EDIF 5
UNIFI DREAM MACHINE 1 / 602232867add	UBIQUITI	06/03/2023	PERMANENTE	RACK 3 EDIF 5
UNIFI DREAM MACHINE 2 / 60223228fad5	UBIQUITI	06/03/2023	PERMANENTE	RACK 3 EDIF 5
SWITCH USW Pro 48 PoE / 784558bad70b	UBIQUITI	27/06/2022	PERMANENTE	RACK 4 EDIF 5
SWITCH USW Pro 48 PoE / 6022329374b4	UBIQUITI	15/03/2023	PERMANENTE	RACK 4 EDIF 5
SWITCH USW Pro 48 PoE / 6022329374b1	UBIQUITI	15/03/2023	PERMANENTE	RACK 4 EDIF 5
SWITCH USW Pro 48 PoE / 60223254fdc5	UBIQUITI	15/03/2023	PERMANENTE	RACK 4 EDIF 5

SWITCH USW Pro 48 PoE / 70a741f94712	UBIQUITI	15/03/2023	PERMANENTE	RACK 4 EDIF 5
SWITCH USW Pro 48 PoE / 70a741f94784	UBIQUITI	15/03/2023	PERMANENTE	RACK 4 EDIF 5
SWITCH EAS-10024T / 0538G-00158	EXTREME	15/07/2006	PERMANENTE	RACK 5 EDIF 5
SWITCH EAS-20048T / 0636G-80708	EXTREME	15/07/2006	PERMANENTE	RACK EDIF 5

INFRAESTRUCTURA EN SITE DRP				
EQUIPO/SERIE	**MARCA**	**FECHA DE ADQUISICION**	**TIPO DE LICENCIAMIENTO**	**UBICACIÓN EN RACK**
NA	NA	NA	NA	NA
NA	NA	NA	NA	NA
NA	NA	NA	NA	NA
NA	NA	NA	NA	NA
NA	NA	NA	NA	NA
NA	NA	NA	NA	NA

12. Anexo 2 – Diagrama de Flujo para Plan de Gestión de Incidentes de Seguridad Informática