GOBIERNO DE SONORA

BOLETÍN OFICIAL

ÓRGANO DE DIFUSIÓN DEL GOBIERNO DEL ESTADO DE SONORA
SECRETARÍA DE GOBIERNO - BOLETÍN OFICIAL Y ARCHIVO DEL ESTADO

Hermosillo, Sonora

Tomo CCXIV

Número 16 Secc. II

Jueves 22 de Agosto de 2024

CONTENIDO

GARMENDIA 157 SUR, COL. CENTRO TELS: 6622 174596, 6622 170556 Y 6622 131286
WWW.BOLETINOFICIAL.SONORA.GOB.MX

LUIS JAVIER ORTEGA, en mi carácter de Subsecretario de Gobierno Digital de la Oficialía Mayor del Gobierno del Estado de Sonora, con fundamento en lo dispuesto por los artículos 71, fracción XVI de la Ley de Gobierno Digital para el Estado de Sonora; y 9, fracción II del Reglamento Interior de la Oficialía Mayor; y

CONSIDERANDO

Que en términos del artículo 9, fracción II del Reglamento Interior de la Oficialía Mayor, la Subsecretaría de Gobierno Digital, tiene la responsabilidad de formular y emitir los instrumentos normativos en materia de seguridad informática que conduzcan a las dependencias, entidades y órganos desconcentrados de la administración pública estatal, en la implementación de estrategias y acciones de seguridad informática.

Que en términos del artículo 71, fracción XVI de la Ley de Gobierno Digital para el Estado de Sonora, la Subsecretaría de Gobierno Digital, tiene la responsabilidad de formular y emitir los lineamientos, medidas efectivas, procedimientos y mecanismos de control para la prevención, detección y corrección de incidentes de seguridad, garantizando la interoperabilidad, el uso correcto de los recursos tecnológicos, la privacidad de los usuarios y la seguridad, protección y uso correcto de la información, asegurando la confidencialidad, integridad y disponibilidad de ésta; así como vigilar su implementación y cumplimiento al interior de los Entes.

Que, en esta era digital, el uso de las tecnologías de la Información y Comunicaciones ha transformado la forma en que las personas interactúan, en el trabajo, estudio, en su vida cotidiana y en el entorno gubernamental. En tal virtud, la atención ciudadana que brinda el Gobierno del Estado de Sonora está siendo dependiente de infraestructuras tecnológicas, a tal grado, que fallas en ellas, pueden causar enormes daños humanos, financieros, e inclusive riesgos a la seguridad de la Entidad.

Que en virtud de lo anterior, a efecto de prevenir y evitar casos de amenazas o ciberataques que pudieran ocasionar un detrimento del patrimonio del Estado de Sonora, así como a la seguridad de la información que detenta el Gobierno con motivo de su interacción con las personas, y con el objeto de establecer acciones para la prevención, detección y corrección de incidentes de seguridad, el uso correcto de los dispositivos informáticos y procurar la confidencialidad, integridad y disponibilidad de la información, es que tengo a bien emitir las siguientes:

MEDIDAS DE PREVENCIÓN, DETECCIÓN Y CORRECCIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

TÍTULO I
CAPÍTULO ÚNICO
DISPOSICIONES GENERALES

PRIMERA. El presente instrumento es de observancia obligatoria para los Entes y tiene por objeto definir las medidas para la prevención, detección y corrección de incidentes de seguridad informática, a efecto de asegurar una respuesta rápida, eficaz y ordenada a los incidentes preservando la confidencialidad, integridad y disponibilidad de la información.

SEGUNDA. Para efectos del presente documento, se entenderá por:

I. **Activo crítico de información:** El activo de información que está clasificado con un nivel de criticidad alta, cuya destrucción, pérdida, alteración o falla tendría un grave impacto o consecuencia en la funcionalidad de la infraestructura de TIC o en los servicios que soporta el Ente.
II. **Activos de información:** Los activos de información pueden ser tangibles o intangibles, es decir elementos de hardware y software, que soportan los servicios esenciales del Ente.
III. **Dispositivos informáticos:** Equipos de cómputo de escritorio o portátil y servidores.
IV. **Entes:** Las dependencias, entidades y órganos desconcentrados de la administración pública estatal.
V. **Incidente de ciberseguridad:** Es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información almacenada y procesada digitalmente.
VI. **Subsecretaría**: La Subsecretaría de Gobierno Digital.
VII. **TIC:** Tecnologías de la Información y Comunicaciones.
VIII. **Utic:** Unidad de Tecnologías de la Información y Comunicaciones u homóloga de las dependencias, entidades y órganos desconcentrados de la administración pública estatal.

TÍTULO II
DE LA PREVENCIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA
CAPÍTULO I
DE LAS MEDIDAS PREVENTIVAS EN GENERAL

TERCERA. Las medidas preventivas consisten en un conjunto de acciones que tienen por objeto reducir la materialización de un incidente que ponga en riesgo la disponibilidad, confidencialidad e integridad de la información almacenada y procesada digitalmente.

CUARTA. Para prevenir la materialización de un incidente de seguridad informática, las personas servidoras públicas, deben observar lo siguiente:

I. Cumplir con las medidas de seguridad contenidas en el presente documento;
II. Abstenerse de desinstalar, deshabilitar, alterar o cambiar el software antivirus instalado por el Ente en los dispositivos informáticos asignados para el desempeño de sus atribuciones;
III. Usar los dispositivos única y exclusivamente para realizar las actividades del puesto que desempeñan, ya sea por disposición normativa o asignadas por el superior jerárquico para alcanzar los objetivos del Ente;
IV. Evitar almacenar o procesar información del Ente en dispositivos informáticos personales;
V. Notificar a su Utic cualquier mensaje de error y/o advertencia que reporte el software de antivirus, respecto de su vigencia, actualizaciones y/o amenazas detectadas;
VI. Notificar inmediatamente a su Utic cuando se tenga conocimiento o sospecha de que alguna de sus contraseñas ha sido vulnerada o comprometida;
VII. Reportar a la Utic de forma inmediata la detección de un correo con posible riesgo o amenaza o cualquier mensaje digital que sea sospechoso;
VIII. Abstenerse de trasladar a otra área del Ente o cambiar de lugar los dispositivos informáticos de escritorio, en caso de que así se requiera, notificarlo a su Utic;
IX. Abstenerse de intentar abrir y/o desarmar los dispositivos informáticos, en caso de falla reportarlo a su Utic;
X. Evitar instalar o usar software que no haya sido previamente autorizado o no cuente con licenciamiento a nombre de la Institución;
XI. Evitar la descarga de mensajes o archivos en redes sociales;
XII. Evitar el uso de redes sociales personales, a menos que el cumplimiento de sus funciones lo amerite;
XIII. Evitar la descarga de software, aplicaciones o actualizaciones poco confiables, no autorizadas, o modificar la configuración estándar del equipo;
XIV. Evitar las visitas a sitios web sospechosos o que no tengan relación con el ejercicio de sus funciones;
XV. Utilizar contraseñas seguras y cambiarlas periódicamente, atendiendo las medidas para la asignación o modificación de contraseñas en dispositivos informáticos que se establecen en el presente instrumento;
XVI. No conectarse a redes públicas gratuitas o poco seguras para realizar las operaciones bancarias sobre cuentas del erario y envío de información sensible;

XVII. Verificar que las direcciones de sitios web que navegan tengan seguridad, es decir, que inicien con https:// y del lado izquierdo y tengan el signo de un candado, esto significa que el sitio web ha sido verificado como auténtico y cumple con los estándares mínimos de seguridad;

XVIII. Abstenerse de Instalar nuevas barras de herramientas de un proveedor desconocido;

XIX. Abstenerse de descargar archivos de música y correos electrónicos desconocidos;

XX. Abstenerse de proporcionar la cuenta de correo electrónico institucional para recibir información que no sea con fines laborales ni compartir la cuenta con otros usuarios;

XXI. Abstenerse de abrir correos electrónicos cuyo remitente sea tu banco, ya que podría tratarse de una página falsa;

XXII. Atender de forma inmediata los comunicados y recomendaciones emitidas por la Utic y/o Subsecretaría sobre seguridad informática;

XXIII. Abstenerse de guardar archivos innecesarios que puedan sobrecargar el disco duro;

XXIV. Mantener al menos el 30% del espacio libre para asegurar un funcionamiento fluido del sistema;

XXV. Apagar el dispositivo informático al término de la jornada laboral, a fin de evitar el sobrecalentamiento;

XXVI. Reiniciar la laptop regularmente para evitar la sobrecarga del sistema y mejorar el rendimiento;

XXVII. Bloquear la sesión en caso de ausentarse temporalmente de su estación de trabajo;

XXVIII. Utilizar accesorios de buena calidad como adaptadores, cargadores y cables que sean compatibles con el dispositivo asignado para evitar dañar los componentes internos;

XXIX. Evitar forzar los puertos al conectar o desconectar dispositivos, cables y periféricos;

XXX. No colocar, sobre y/o cerca de los equipos y sus periféricos, alimentos o bebidas, ni consumirlos mientras los operan;

XXXI. Colocar los equipos portátiles en un lugar libre de polvo;

XXXII. No obstruir las ranuras de ventilación, los equipos portátiles no deben ser colocados sobre las piernas cuando estén encendidos; y

XXXIII. Las demás que se establezcan en este instrumento y demás disposiciones jurídicas aplicables.

Las personas servidoras públicas que trabajan vía remota son responsables de la seguridad y privacidad de la información y los datos que manejan de manera digital. Cuando cuenten con equipo de cómputo propiedad del Ente, deberán atender las medidas de seguridad informática antes descritas, así como procurar conectarse a una red segura. Si el equipo es personal, procurará crear una sesión independiente

de trabajo en sus activos a efecto de garantizar la seguridad y privacidad de la información digital que posean para el desarrollo de sus actividades.

QUINTA. Para prevenir la materialización de un incidente de seguridad informática, las Utic deben observar los siguiente:

I. Difundir y vigilar al interior de su Ente el cumplimiento de las presentes medidas, así como su Plan para la Gestión de Incidentes de Seguridad Informática;
II. Instalar en todos los dispositivos informáticos del Entre software antivirus;
III. Mantener sistemas y software actualizados;
IV. Mantener los dispositivos informáticos actualizados tanto en su sistema operativo como el software instalado, aplicando los parches, actualizaciones y service packs una vez que estos se encuentren disponibles y fuera de período de prueba;
V. Configurar los dispositivos informáticos para que entren en modo de suspensión o hibernación cuando no estén en uso durante periodos prolongados, con el propósito de conservar la energía de la batería y prolongar su vida útil;
VI. Difundir y asesorar a las personas servidoras públicas del Ente, sobre las recomendaciones del fabricante de los dispositivos informáticos para su cuidado, a fin de maximizar su vida útil;
VII. Atender los reportes de fallas de dispositivos informáticos;
VIII. Asesorar a los servidores públicos del Ente sobre las presentes medidas para prevenir la ocurrencia de incidentes;
IX. Elaborar y someter a consideración del titular de su Ente el Plan para la Gestión de Incidentes de Seguridad Informática;
X. Ejecutar su Plan para la Gestión de Incidentes de Seguridad Informática ante un incidente que provoque interrupción, alteración, daño, destrucción o pérdida de la información.
XI. Manifestar al área correspondiente las necesidades de antivirus y realizar las gestiones necesarias para su adquisición;
XII. Difundir, orientar y enviar recordatorios trimestrales sobre el uso de contraseñas seguras y su cambio periódico, atendiendo las medidas para la asignación o modificación de contraseñas en dispositivos Informáticos que se establecen en el presente instrumento;
XIII. Contar con una relación de las personas servidoras públicas que cuentan con correo electrónico institucional;
XIV. Informar de forma inmediata a los servidores públicos adscritos al Ente, de los comunicados y recomendaciones emitidas por la Subsecretaría sobre seguridad informática y en su caso, brindar el soporte técnico requerido;
XV. Capacitar al personal en prácticas de seguridad informática; y
XVI. Las demás que se establezcan en este instrumento y demás disposiciones jurídicas aplicables.

SEXTA. Para prevenir la materialización de un incidente de seguridad informática, los Entes deben observar los siguiente:

I. Aprobar su Plan para la Gestión de Incidentes de Seguridad Informática y garantizar su implementación;
II. Atender de forma inmediata los comunicados y recomendaciones emitidas por su Utic o la Subsecretaría sobre seguridad informática;
III. Reportar a la Utic, los incidentes de seguridad informática que se presenten;
IV. Proveer y gestionar los recursos financieros, humanos y materiales requeridos por su Utic para dar cumplimiento al presente instrumento normativo y garantizar la seguridad de la información almacenada y procesada digitalmente; y
V. Las demás que se establezcan en este instrumento y demás disposiciones jurídicas aplicables.

SÉPTIMA. En la asignación o cambio de contraseñas en dispositivos informáticos, se deberá tomar en consideración, al menos, las siguientes medidas:

I. Contar con una longitud mínima de 16 caracteres;
II. Incluir, por lo menos, una letra mayúscula, una letra minúscula, un símbolo especial y un número, evitando el uso de nombres y frases;
III. Verificar que sean únicas e irrepetibles, evitando el uso de palabras comunes o datos personales o contenido de identificadores de recurso informático;
IV. Ser renovadas en lapsos no mayores a 90 días; y
V. La misma contraseña no deberá de ser empleada en diferentes recursos (ejemplo: acceso a NAS, SAN, Router, Switch, Servidores Físicos, Virtuales, correo electrónico, cuentas bancarias personales e institucionales, bases de datos, aplicativos, y/o carpetas compartidas).

CAPÍTULO II
DE LAS MEDIDAS PREVENTIVAS PARA CENTROS DE DATOS

OCTAVA. Las Utic´s de los Entes con Centros de datos, además de atender las medidas preventivas generales descritas en el presente instrumento, éstas deberán:

I. Implementar controles de accesos a los sistemas de información, asignando identificaciones únicas para los usuarios, que les permita estar vinculados a sus acciones y mantener la responsabilidad por ellas, para lo cual:

a. Deberán contar con una relación actualizada de las personas servidoras públicas que tienen acceso autorizado a los sistemas y procedimientos que permitan la identificación y autenticación para dicho proceso;
b. Deberán contar con un mecanismo que permita la identificación, de forma inequívoca y personalizada, de toda aquella persona que intente acceder al sistema y la verificación de que está autorizada; y
c. El titular de la Utic deberá ser el único con permiso para conceder, alterar o anular la autorización para el acceso a los sistemas.

II. Establecer un control de acceso para sistemas móviles o portátiles conectados a la red del Ente;
III. Deshabilitar y/o retirar inmediatamente los derechos de acceso del personal y terceros a los recursos de tecnologías de la información (datos, sistemas de aplicación, instalaciones, tecnología, y demás aplicables) después de que se formalice la terminación de la relación laboral o contractual con el Ente, o bien, sean actualizados en función del cambio de su situación laboral o contractual;
IV. Hacer uso de diferentes técnicas de cifrado para proteger y garantizar la autenticidad, confidencialidad e integridad de la información almacenada y procesada digitalmente;
V. Implementar protección física contra desastres naturales, ataques maliciosos o accidentes;
VI. Establecer el perímetro de seguridad con una barrera física, para proteger las instalaciones de procesamiento de información;
VII. Eliminar de forma segura la información sensible y licencias de software de los equipos que causarán baja o reasignación;
VIII. Verificar el estado físico del cableado;
IX. Realizar copias de seguridad periódicas de los activos críticos de información, utilizando la opción que más convenga al Ente, ya sea en una unidad externa, en Discos Duros de Estado Sólido o en la nube;
X. Almacenar de manera separada la base datos de operación y la base de datos de respaldo;
XI. Buscar medidas alternas de almacenamiento de respaldo;
XII. Inventariar y actualizar los activos de información periódicamente;
XIII. Monitorear la carga de los servidores y switches, el ancho de banda utilizado en la red, el espacio usado en servidores, las conexiones en firewall y antispam y conexiones en servidores y switches;
XIV. Informar oportunamente al titular del Ente y a la Subsecretaría cualquier incidente o riesgo en el cual se vea afectada la información o los datos del Ente almacenados y procesados digitalmente;
XV. Asesorar y apoyar a las personas servidoras públicas adscritas al Ente, en el procedimiento para realizar el respaldo de la información guardada en la nube de ONEDRIVE, con base en lo establecido en el Anexo 1 de este instrumento; y
XVI. Las demás que se establezcan en este instrumento y demás disposiciones jurídicas aplicables.

NOVENA. Las personas servidoras públicas que desempeñan un rol en el Centro de Datos del Ente, son responsables de la seguridad y privacidad de la información que manejan en sus activos con sus identificaciones, por lo que además de atender las medidas preventivas generales descritas en el presente instrumento, deben observar lo siguiente:

I. Informar oportunamente a la persona titular de la Utic cualquier incidente o riesgo en el cual se vea afectada la información o los datos del Ente;
II. Abstenerse de compartir o autorizar el uso de identificaciones únicas, asignadas para los accesos a sistemas de información; y
III. Las demás que se establezcan en este instrumento y demás disposiciones jurídicas aplicables.

DÉCIMA. Cuando los Entes cuenten con Centros de Datos, además de atender las medidas preventivas generales descritas en el presente instrumento, éstos deberán:

I. Garantizar la implementación de las medidas de seguridad físicas y lógicas para proteger los componentes de los Centros de Datos contra cualquier amenaza y garantizar la continuidad de sus operaciones;
II. Asegurarse de renovar las cartas convenio de servicio de servidores virtuales, en el caso de que su información se encuentre hospedada en el centro de datos del Gobierno del Estado;
III. Verificar la ejecución del Plan para la Gestión de Incidentes de Seguridad Informática, en caso de presentarse algún incidente de seguridad que ponga en riesgo la información almacenada y procesada digitalmente o la continuidad de los servicios esenciales del Ente; y
IV. Las demás que se establezcan en este instrumento y demás disposiciones jurídicas aplicables.

TÍTULO III
CAPÍTULO ÚNICO
DE LA PLANIFICACIÓN PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

DÉCIMA PRIMERA. Cada Ente, incluyendo los que tienen su información hospedada en el Centro de Datos de la Subsecretaría, deberán contar con un Plan para la Gestión de Incidentes de Seguridad Informática, el cual deberá estar alineado a sus necesidades con base en sus objetivos estratégicos, actividades y servicios esenciales y a la información que posean o generen.

El objetivo del Plan para la Gestión de Incidentes de Seguridad Informática es generar un esquema de acciones que permita preservar la información y restaurar los servicios

esenciales del Ente lo más pronto posible, ante la ocurrencia de un incidente de seguridad informática, minimizando su impacto. El titular del Ente deberá aprobar su Plan para la Gestión de Incidentes de Seguridad Informática dentro de los 30 días hábiles posteriores a la entrada en vigor del presente instrumento y deberá ser remitido a la Subsecretaría dentro de dicho periodo, para que ésta pueda elaborar una base de datos de los responsables de la ejecución de dichos Planes, y poder acompañar al Ente en caso de un incidente clasificado como "Crítico", "Muy Alto" o "Alto".

En caso de presentarse algún cambio en el contenido y/o datos generales del responsable de la ejecución del Plan para la Gestión de Incidentes de Seguridad Informática, se deberá hacer de conocimiento a la Subsecretaría, en un término de diez días posteriores al cambio realizado.

Los Entes deberán elaborar su Plan para la Gestión de Incidentes de Seguridad Informática considerando, al menos, lo establecido en las siguientes etapas:

A. PREPARACIÓN

I. El Plan deberá contener los datos generales de la persona servidora pública designada como responsable de su ejecución y actualización, que a continuación se señalan:
   a. Nombre completo
   b. Puesto que desempeña
   c. Correo institucional
   d. Número de teléfono celular

II. Se recomienda crear un equipo de atención de incidentes de seguridad, que se encargue de realizar la atención, definir los procedimientos y la clasificación de incidentes. En este caso, se deben asignar los roles y responsabilidades de los integrantes y capturar los datos generales que se enlistan en la fracción anterior.

III. Identificar e inventariar sus procesos y activos de información considerando al menos:

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

Los tipos de activos pueden comprender: Información, Equipos/ Sistemas/ Infraestructura, Redes de Telecomunicaciones, Procesos, Servicios, Recursos humanos y equipamiento auxiliar.

IV. Clasificar sus activos de información almacenada y procesada digitalmente de acuerdo con su nivel criticidad, tomando en consideración las tres propiedades de la información: confidencialidad, integridad y disponibilidad, de acuerdo con los siguientes criterios de criticidad:

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.

V. Elaborar una matriz de gestión de riesgos basado en la clasificación de sus activos de información almacenada y procesada digitalmente, que permita identificar las vulnerabilidades y riesgos a los que se enfrentan dichos activos, permitiendo establecer controles más adecuados en temas de seguridad.

VI. Identificar los diversos incidentes que podrían impactar la continuidad de las operaciones, así como sus repercusiones financieras, humanas, de reputación, entre otras.

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

VIII. Definir la protección y respaldo de la información almacenada y procesada digitalmente, incluyéndome al menos:

- El tipo de respaldo que realizan, es decir, si es incremental, parcial o total;
- La información que respaldan;
- La periodicidad con que lo hacen;
- Los medios de respaldo que utilizan, es decir, unidad externa, Discos Duros de Estado Sólido o la nube;
- Las medidas alternas de almacenamiento;
- Ubicación donde se encuentra almacenada la base datos de operación y la base de datos de respaldo.

IX. Establecer los canales de comunicación a través de los cuales se podrá comunicar cualquier alerta que implique la ocurrencia de un incidente.

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.

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

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.

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.

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.

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

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 min
Medio	15 min
Bajo	5 min

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

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.**

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".

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.

TÍTULO IV
CAPÍTULO ÚNICO
DE LAS RESPONSABILIDADES ADMINISTRATIVAS

DÉCIMA TERCERA. El incumplimiento del presente instrumento normativo por parte de los servidores públicos que integran los Entes, será causa de responsabilidades administrativas en los términos que establece la Ley de Responsabilidades y Sanciones para el Estado de Sonora, sin perjuicio de las demás que pudieran resultar de la inobservancia o violación de otras disposiciones jurídicas aplicables.

DÉCIMA CUARTA. El incumplimiento de las obligaciones en materia de manejo de datos personales, será causa de sanción conforme lo establece la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de Sonora.

TRANSITORIOS

PRIMERO. Publíquese en el Boletín Oficial del Gobierno del Estado de Sonora para su debida observancia y aplicación.

SEGUNDO. El presente instrumento entrará en vigor el día hábil siguiente al de su publicación.

Dado en Hermosillo, Sonora, a los 14 días del mes de agosto de dos mil veinticuatro.

LUIS JAVIER ORTEGA CISNEROS
SUBSECRETARIO DE GOBIERNO DIGITAL
DE LA OFICIALÍA MAYOR DEL GOBIERNO
DEL ESTADO DE SONORA

ANEXO 1

PROCEDIMIENTO PARA CONFIGURAR ONEDRIVE PARA SOLO SUBIDA DE RESPALDOS EN LA NUBE EN SERVIDORES LINUX UBUNTU 22.04

La realización de respaldos de información de manera periódica sirve para garantizar que la información almacenada en los dispositivos informáticos no se afecte con alguna falla y esto se traduzca, a su vez, en una vulneración de la información.

Las áreas de sistemas del Gobierno del Estado de Sonora que cuenten con servidores Linux, podrán configurar el respaldo de servidores en OneDrive y sincronizar una carpeta única de respaldo a cada servidor en el sistema operativo Ubuntu 22.04.

Las carpetas únicas de respaldo hacia la nube de OneDrive serán usadas sólo en la modalidad de subida, cada servidor podrá contar con una carpeta de respaldo aislado, sin que se descarguen otros archivos o carpetas ajenos a los que específicamente se elijan.

Es necesario contar con el cliente de OneDrive previamente instalado, así como algún editor de texto, tener a la mano las credenciales de acceso a la cuenta institucional del Gobierno del Estado de Sonora y el cliente OneDrive no debe estar autorizado para sincronización de archivos.

Los pasos para lograr la configuración del cliente de OneDrive para definir que cada servidor se limite a guardar información en la carpeta que se decida son los siguientes:

1. Desde la terminal de consola, ejecutar un editor de texto para crear el siguiente archivo, en este caso se usará nano:

```
$ nano ~/.config/onedrive/sync_list
```

Dicho archivo debe guardarse con el siguiente contenido:

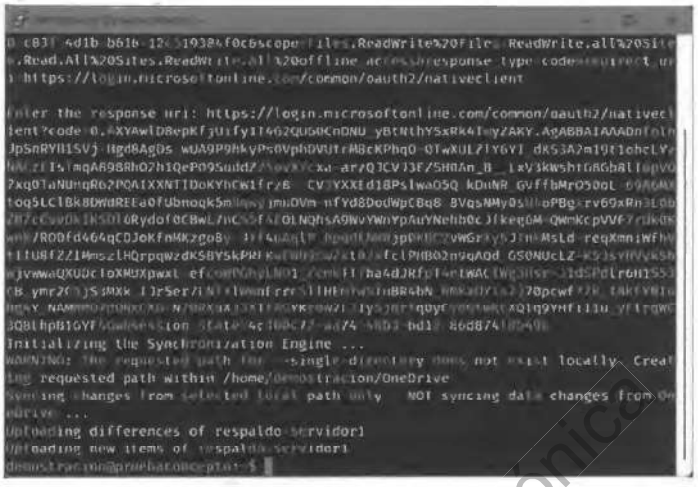
!/*
/respaldo-servidor1

Proceder a guardar el archivo.

2. Ejecutar el siguiente comando para preconfigurar el cliente de OneDrive e iniciar el proceso de autorización:

$ onedrive --resync --synchronize --no-remote-delete --single-directory respaldo-servidor1

Completar el intercambio de autorización, así como lo describe el paso 4 y 5 del Procedimiento de respaldo de servidores Linux a OneDrive (PSRL-01).



3. Confirmar que la carpeta remota que se eligió para guardar los respaldos esté creada dentro de la carpeta de OneDrive mediante el comando ls:
ls ~/OneDrive