ÍNDICE

		Página
I.	OBJETIVO	2
II.	ALCANCE	2
III.	FUNDAMENTO LEGAL	2
IV.	DEFINICIONES	2
V.	POLÍTICAS	3
VI.	ANEXOS	8
VII.	CONTROL DE CAMBIOS	9
VIII.	FIRMA DE AUTORIZACIÓN DEL DOCUMENTO	9

I. OBJETIVO

Establecer las directrices para gestionar la seguridad informática, con la finalidad de procurar la protección de los Habilitadores Tecnológicos que intervienen en la operación de las Dependencias y Entidades del Gobierno del Estado de Yucatán.

II. ALCANCE

Aplica al personal adscrito a la Subsecretaría de Tecnologías de la Información y Comunicaciones de la Secretaría de Administración y finanzas, así como a las Dependencias y Entidades de la Administración Pública Estatal que en su operación intervengan o estén involucrados habilitadores tecnológicos.

III. FUNDAMENTO LEGAL

Ámbito Federal

Artículo 6, apartado A, fracción I; de la Constitución Política de los Estados Unidos Mexicanos.

Ámbito Estatal

Artículo 26, fracción IX; de la Ley para la Igualdad entre Mujeres y Hombres del Estado de Yucatán

Artículo 26, fracción IX; de la Ley para la Igualdad entre Mujeres y Hombres del Estado de Yucatán

Título IV, capítulo II; artículo 31, fracción XIII del Código de la Administración Publica de Yucatán.

Artículo 11, apartado A, fracción XIX del Reglamento del Código de la Administración Publica de Yucatán.

Artículo 66, fracción I, IV, V, VI, VIII, y X del Reglamento del Código de la Administración Publica de Yucatán.

IV. DEFINICIONES

Acceso: Permiso otorgado para la interacción con habilitadores tecnológicos de forma física o digital, acorde a las necesidades de operación del usuario asignado.

Activos Digitales: Llámese a cualquier bien que existe, contiene, genera o gestiona información en formato digital.

Componentes Tecnológicos: Llámese así a las herramientas e infraestructura de tecnologías de la información y comunicaciones utilizadas en la operación y entrega de servicios de una Dependencia o Entidad. Estos pueden ser cualquier dispositivo informático o de comunicación.

Estrategias de Tecnologías: Son directrices establecidas por la Subsecretaría de Tecnologías y Comunicaciones que sirven como marco referencial para alinear las acciones de la operación tecnológica del Gobierno del Estado con el Plan Estatal de Desarrollo.

Dueño de la Información: Persona o grupo de personas pertenecientes a una Unidad Administrativa con la atribución de definir el uso y resguardo de la información generada o recopilada en un Habilitador Tecnológico.

Habilitadores Tecnológicos: Es el conjunto de los Activos Digitales y Componentes Tecnológicos que interactúan en la operación y entrega de servicios del Gobierno del Estado

Plan de Recuperación ante Desastres (DRP): Conjunto de políticas, herramientas y procedimientos para permitir la recuperación o continuidad de los servicios tecnológicos claves para la organización después de un desastre natural o contingencia.

Riesgo: Toda circunstancia o situación que aumenta las probabilidades de que un servicio presente una degradación.

STIC: Subsecretaría de Tecnologías de la Información y Comunicaciones.

V. POLÍTICAS

Políticas Generales

1. Las presentes políticas son aprobadas por el titular de la de la Subsecretaría de Tecnologías de la Información y Comunicaciones (STIC) en cumplimiento del Reglamento del Código de la Administración Pública de Yucatán.
2. La operación de las Dependencias y Entidades del Gobierno del Estado deben contemplar las acciones de seguridad basadas en el M-PL-GSI-01 Modelo de Seguridad Informática definido por la STIC.
3. El M-PL-GSI-01 Modelo de Seguridad Informática establecido por la STIC contempla la implementación de las etapas Gobernar, Identificar, Proteger, Detectar, Responder y Recuperarse, en la gestión de los Habilitadores Tecnológicos involucrados en la operación clave de las Dependencias y Entidades del Gobierno del Estado.
4. Se debe considerar el uso de las herramientas propuestas para cada etapa del M-PL-GSI-01 Modelo de Seguridad Informática de acuerdo a la pertinencia y casos de uso.
5. Las situaciones no previstas en las presentes políticas serán resueltas por el titular de la STIC.
6. Las presentes políticas entran en vigor al día siguiente de su aprobación y publicación.

Políticas Especificas

1. Prevenir Riesgos
   1.1. Para Prevenir Riesgos en los Habilitadores Tecnológicos, los controles de seguridad deben considerar instrumentos y mecanismos que permitan Identificar los recursos tecnológicos de una Dependencia o Entidad, la trazabilidad en la interacción con sus usuarios y Proteger a través de medidas que mitiguen su degradación durante la operación de las Dependencias o Entidades.
   1.2. Los controles de seguridad para prevenir riesgos en los Habilitadores Tecnológicos se clasifican en Registro, Autenticación y Planeación.
   1.3. Controles de Registro
      1.3.1. Los controles de Registro tienen como objetivo identificar y gestionar la información de los recursos tecnológicos con los que cuenta una Dependencia o Entidad, considerando los Habilitadores Tecnológicos y sus características.

1.3.2. Los controles de Registro de los Habilitadores Tecnológicos deben realizarse a través de controles de Inventarios que contengan la información de los Activos Digitales y Componentes Tecnológicos de una Dependencia o Entidad.

1.3.3. Los Inventarios de los Activos Digitales deben considerar el control de sus actualizaciones y accesos, alineado al PL-STI-DDP-01 Política para Gestionar Plataformas Digitales.

1.3.4. Los Inventarios de los Componentes Tecnológicos deben considerar la información que describa su estado y disponibilidad, con base en su ciclo de vida descrito en la PL-STI-DGT-02 Política para Regular los Habilitadores Tecnológicos del Gobierno del Estado.

1.3.5. El registro de los habilitadores tecnológicos debe realizarse posterior a culminar la etapa de Obtención, alineado a la PL-STI-DGT-02 Política para Regular los Habilitadores Tecnológicos del Gobierno del Estado.

1.3.6. Los Habilitadores Tecnológicos registrados en inventarios deben estar relacionados con al menos un servicio de la Dependencia o Entidad identificado en el F-PL-GST-01 Catálogo de Servicios de TI de acuerdo a las PL-STI-DTD-03 Políticas para Gestionar Servicios de TI.

1.3.7. El responsable de la Unidad Informática debe realizar acciones que procuren la integridad de los Habilitadores Tecnológicos en controles de inventarios, con medidas de planeación, evaluación y administración de riesgos a los que están expuestos los Habilitadores Tecnológicos, de acuerdo a las políticas PL-STI-DTD-01 Política para Alinear Estrategias de Control de la Operación Tecnológica del Gobierno del Estado, en su apartado del Control de Riesgos Tecnológicos.

1.4. Controles de Autenticación

1.4.1. Los controles de Autenticación tienen como objetivo conocer la trazabilidad de la interacción de usuarios, de acuerdo a sus Accesos, con los Habilitadores Tecnológicos de una Dependencia o Entidad, así como de los elementos relacionados a estos.

1.4.2. La información considerada para los controles de Autenticación debe ser definida por los Especialistas Técnicos, con base en el C-PL-GEI-01 Catálogo de Habilitadores Tecnológicos.

1.4.3. Los Controles de Autenticación deben partir de la relación de Usuarios de un Habilitador Tecnológico, sus perfiles y permisos otorgados a través de una Credencial de acceso.

1.4.4. Los accesos a Habilitadores Tecnológicos y los espacios donde se almacenan deben ser autorizados por el responsable superior de una Unidad Administrativa.

1.4.5. Los controles de Autenticación relacionados con el intercambio de información automatizado entre Activos Digitales deben considerar el uso de Interfaces de Programación de Aplicaciones (API), librerías y demás Software de Sistemas, acordadas entre los Responsables Técnicos involucrados, para su gestión y control, solicitados a través del F-PL-GSI-01 Solicitud de Alta de Servicio en la Capa de Seguridad.

1.4.6. Los controles de Autenticación deben realizarse a través de instrumentos de Bitácoras que contemplen el seguimiento a las acciones de los usuarios en los Habilitadores Tecnológicos de las Dependencias y Entidades.

1.4.7. El resguardo de las bitácoras generadas son responsabilidad de los Encargados de los Habilitadores Tecnológicos que los generan.

1.5. Controles de Planeación

1.5.1. Los controles de Planeación consideran el conjunto de medidas previstas para las Plataformas Digitales, su estructura de Información y los Componentes Tecnológicos con los que se involucran, para su integración.

1.5.2. Los controles de Planeación para las Plataformas Digitales deben alinearse a lo descrito en la PL-STI-DDP-01 Política para Gestionar Plataformas Digitales del Gobierno del Estado.

1.5.3. Los controles de Planeación para las estructuras de Información deben alinearse a lo descrito en la PL-STI-DED-01 Política para Administrar Bases de Datos.

1.5.4. Los controles de Planeación para los Componentes Tecnológicos deben alinearse a lo descrito en la PL-STI-DGT-02 Política para Regular los Habilitadores Tecnológicos del Gobierno del Estado.

1.5.5. Las Dependencias y Entidades del Gobierno del Estado deben planificar el ciclo de atención a un desastre y documentarlo en un Plan de Recuperación ante Desastres (DRP) de acuerdo a las políticas PL-STI-02 Política para Regular los Planes de Recuperación ante Desastres del Gobierno del Estado.

1.5.6. Las Unidades Informáticas deben establecer acciones que permitan dar a conocer y concientizar al personal de su Dependencia o Entidad las medidas que faciliten el entendimiento y la adopción de la seguridad informática.

1.5.7. Cualquier particularidad relacionada con la protección de los Habilitadores Tecnológicos que presente una Dependencia o Entidad debe ser notificada a la STIC para determinar las acciones pertinentes.

1.6. Protección de Activos Digitales

1.6.1. Las Dependencias y Entidades deben llevar a cabo acciones de control para los Activos Digitales y Componentes Tecnológicos relacionados con su operación, con base en el M-PL-GSI-01 Modelo de Seguridad Informática establecido por la STIC.

1.6.2. La protección para los Activos Digitales tales como plataformas, bases de datos, repositorios digitales, tecnologías de telepresencia o cualquier otro que considere intercambio o almacenamiento de información, deben establecer controles basados en niveles de permisos, utilizando múltiple factor de autenticación siempre que sea posible.

1.6.3. La protección de Componentes Tecnológicos y el espacio destinado para estos, tales como centros de datos o espacios tecnológicos restringidos, almacenes de refacciones tecnológicas, equipos especializados o cualquier otro que deba ser operado por

especialistas técnicos, deben contar con controles de acceso que identifiquen al personal autorizado para su ingreso y el alcance de sus acciones.

1.6.4. Las plataformas digitales creadas por las Dependencias y Entidades del Gobierno del Estado, debe cumplir las recomendaciones establecidas por la STIC en la G-PL-GSI-01 Medidas de Seguridad para Plataformas Digitales.

1.6.5. La interacción de los usuarios con las plataformas digitales debe estar protegida a través de medidas que controlen su acceso y la clasificación del tipo de usuarios y permisos de interacción que tendrán con dicha plataforma digital, de acuerdo lo establecido en la PL-STI-DDP-01 Política para Gestionar Plataformas Digitales del Gobierno del Estado.

1.6.6. El resguardo de los accesos, así como la actividad realizada a través de ellos, son responsabilidad de los Usuarios a quien fueron asignados.

1.6.7. Las Dependencias y Entidades que administren sus bases de datos deben establecer técnicas, herramientas y métricas para la correcta gestión de la seguridad de los datos alineado a estás políticas.

1.6.8. Las técnicas para la seguridad de datos deben contemplar la regulación de accesos, la nomenclatura de usuarios y contraseñas, la autenticación, prácticas y reglas de autorización.

1.6.9. El responsable de la Administración de una base de datos debe asegurar cambiar la configuración por defecto de los motores de las bases de datos durante la instalación y configuración, así como la instalación y configuración de las herramientas de software y hardware de control de riesgos para la operación de la base de datos.

1.6.10. El administrador de base de datos es responsable de determinar los parámetros de tolerancia en cuanto a accesos a las bases de datos, para realizar el análisis correspondiente que determine la naturaleza de estas alertas.

1.6.11. Las Dependencias y Entidades deben garantizar que solo los usuarios autorizados accedan a las bases de datos apoyados de herramientas o tareas de monitoreo, validadas por la STIC.

1.6.12. Los accesos a las bases de datos de una Dependencia o Entidad deben regirse bajo un estricto control, estableciendo la relación de los tipos de usuario y los permisos otorgados a estos para su operación.

1.6.13. Los tipos de usuario que se pueden asignar son Usuario Administrador, Usuario de la Base de Datos y Usuario de Aplicación.

1.6.14. Se debe considerar "Usuario Administrador" a quien se le otorgue control total sobre el motor de base de datos y sobre todos los objetos de la base de datos, solo debe ser de conocimiento del Administrador de Base de Datos. Se le deben otorgar permisos *"sysadmin"* y es el usuario por defecto que viene embebido en el motor de la base de datos al momento de instalarse y está bajo la responsabilidad del Administrador de Bases de Datos.

1.6.15. Se deben considerar como "Usuario de la Base de Datos" a los usuarios solicitados que cuenten con permisos de lectura de los objetos en las bases de datos. Se le deben

otorgar permisos mínimos los cuales permiten efectuar las acciones requeridas en su operación.

1.6.16. Se deben considerar como "Usuario de Aplicación" a las cuentas que son utilizadas por sistemas para la interacción entre el servidor de aplicaciones y la base de datos. Se le deben otorgar permisos para consulta, modificación, actualización o eliminación de información y se crean de manera local en el motor de base de datos. Este tipo de usuario no debe ser utilizado para otros fines que no sean los que se indican en este punto.

1.6.17. Los permisos sólo pueden ser actualizados a los "Usuarios de Aplicación", no se pueden asignar permiso de escritura a "Usuarios de Base de Datos", sin embargo, a los Usuarios de Base de Datos sí se les puede conceder permisos de lectura a nuevos objetos de base de datos.

1.6.18. La nomenclatura para los nombres y contraseñas de los usuarios de las bases de datos debe alinearse a las especificaciones del motor de la base de datos siendo: establecido en la guía G-PL-ABD-01 Manual de Buenas Prácticas de Bases de Datos.

1.6.19. La autorización para la creación de usuarios a una base de datos debe considerar que:

- El usuario deberá presentar el formato F-PL-ABD-01 Formato de Solicitud de Usuario Base de Datos.
- Si la cuenta de base de datos fue heredada, el jefe del departamento deberá de dar aviso por correo al área de Administración de Base de Datos y Estrategia de Datos para el cambio inmediato de la contraseña de la cuenta.
- No se permite la solicitud de usuarios con permiso de administrador.
- En el formato de solicitud de usuario se debe de especificar los objetos y permisos a asignar para cada objeto de base de datos.

1.6.20. El Administrador de Base de Datos debe programar las herramientas de Auditoría de Base de Datos propia del motor de la base, considerando cubrir los accesos (login), cambios a nivel estructura (DDL) y los cambios a nivel datos (DML), los periodos de inicio y fin de la auditoría y el tiempo de retención de los archivos generados por la tarea según acuerdos entre el Administrador de la Base de Datos y la Dependencia y Entidad dueña de la información.

1.6.21. Los Repositorios Digitales utilizados en el Gobierno del Estado deben seguir las especificaciones recomendadas por la STIC para adecuarse al tipo de información definida para su resguardo.

1.6.22. Las Dependencias y Entidades son responsables de definir los usuarios que tendrán acceso a los Repositorios Digitales y sus permisos, así como la información que reguardarán.

1.6.23. Es responsabilidad del Encargado de la Unidad Informática de una Dependencia o Entidad gestionar la obtención y/o accesos a los Repositorios Digitales a utilizar por su Dependencia o Entidad, así como monitorear su estado, capacidades y buen uso.

1.6.24. Los usuarios son responsables del uso de los Repositorios Digitales y la información aprobada para resguardar, al alcance de sus permisos.

1.6.25. El tipo de información aprobada para resguardar en un Habilitador Tecnológico del Gobierno del Estado no puede ser extraída o compartida sin autorización previa del Dueño de la Información.

2. Para atender eventos
   2.1. Las Unidades Informáticas deben realizar el monitoreo y/o auditorías internas del funcionamiento de los Habilitadores Tecnológicos con los que cuenta la Dependencia o Entidad, que ayuden a Detectar y Responder ante vulnerabilidades en la operación de las Dependencias y Entidades del Gobierno del Estado.
   2.2. Para Detectar vulnerabilidades las Unidades Informáticas deben monitorear y/o realizar auditorías internas del funcionamiento de los Habilitadores Tecnológicos de forma continua, apoyado de herramientas especializadas o mecanismos aprobados por la STIC.
   2.3. Los controles de seguridad deben apoyar a detectar situaciones que vulneren la operación de las Dependencias y Entidades, identificando los riesgos asociados y dimensionando el impacto que ocasiona, alineado a la PL-STI-DTD-01 Política para Alinear Estrategias de Control de la Operación Tecnológica del Gobierno del Estado.
   2.4. El impacto dimensionado se puede clasificar como impacto controlado o impacto crítico.
   2.5. El Impacto Controlado considera la integración de instrumentos y mecanismos para atender las situaciones planificadas y mantener la continuidad de los Habilitadores Tecnológicos en la Operación.
   2.6. Cualquier situación detectada debe ser atendida por la Unidad Informática de la Dependencia o Entidad y en caso de ser necesario, solicitar apoyo a la STIC a través del procedimiento PR-DGT-SOP-01 Procedimiento para Atender Solicitudes de Servicios de TI, para determinar la directriz de las acciones a realizar.
   2.7. El impacto crítico considera las situaciones imprevistas derivadas de un evento que detengan la operación de los Habilitadores Tecnológicos.
   2.8. Las Dependencias y Entidades son responsables de planificar acciones que atiendan posibles eventos con impacto crítico, documentándolas como acciones de mitigación en un Plan de Recuperación ante Desastres (DRP) de acuerdo a la política PL-STI-02 Política para Regular los Planes de Recuperación ante Desastres del Gobierno del Estado.
   2.9. Las Dependencias y Entidades son responsables de actualizar y mejorar las acciones de mitigación y recuperación consideradas en su Plan de Recuperación ante Desastres de acuerdo a lo establecido en las políticas PL-STI-02 Política para Regular los Planes de Recuperación ante Desastres del Gobierno del Estado.
3. Recuperar Operación
   3.1. Las Unidades Informáticas de las Dependencias y Entidades del Gobierno del Estado son responsables de restablecer la operación de los habilitadores tecnológicos que intervienen en sus servicios clave derivado de un evento que impida su continuidad, ejecutando las acciones de recuperación documentadas en su Plan de Recuperación ante Desastres de

acuerdo a la política PL-STI-02 Política para Regular los Planes de Recuperación ante Desastres del Gobierno del Estado.

3.2. Para Restablecer la Operación de los Habilitadores Tecnológicos deben contemplar la integridad de las estructuras de Información, la funcionalidad de los Componentes Tecnológicos, la disponibilidad de las Plataformas Digitales y el Acceso de los usuarios.

3.3. Para Restablecer la integridad de las estructuras de Información deben considerar los instrumentos y mecanismos descritos en la PL-STI-DED-01 Política para Administrar Bases de Datos.

3.4. Para Restablecer las funcionalidades de los Componentes Tecnológicos deben considerar los criterios de operación de los Servicios de TI con los que se relacionan y los riesgos técnicos que implica su exposición, alineado a la PL-STI-DTD-03 Política para Gestionar Servicios de TI.

3.5. Para Restablecer la disponibilidad de las Plataformas Digitales deben realizarse de forma gradual considerando la exposición al riesgo que representa y el impacto de su materialización, tomando en cuenta las acciones pertinentes de la PL-STI-DDP-01 Política para Gestionar Plataformas Digitales del Gobierno del Estado.

3.6. Para Restablecer el Acceso de los Usuarios a los Habilitadores Tecnológicos deben considerar los perfiles, funciones y servicios donde interactúen para determinar los criterios de prioridad, alineado al PR-STI-07 Procedimiento para Gestionar el Acceso de Usuarios a Habilitadores Tecnológicos

3.7. El responsable de la Unidad Informática debe informar los resultados derivados de la ejecución del Plan de Recuperación ante Desastres y/o las propuestas de mejoras requeridas en el plan para su análisis, acuerdos y acciones requeridas, ya sea en alguna sesión del Comité de Enlace de su Dependencia o Entidad o a través de medios acordados.

3.8. Las Dependencias y Entidades son responsables de actualizar y mejorar las acciones de recuperación consideradas en su Plan de Recuperación ante Desastres de acuerdo a lo establecido en las políticas PL-STI-02 Política para Regular los Planes de Recuperación ante Desastres del Gobierno del Estado.

VI. ANEXOS

Código	Nombre del anexo	Ubicación	AT	AC	PTC	Disposición final
M-PL-GSI-01	Modelo de Seguridad Informática del Gobierno del Estado	SIN	Indefinido	5 años	5 años	Eliminar
F-PL-GSI-01	Solicitud de Alta de Servicio en la Capa de Seguridad	SIN	2 años	5 años	7 años	Eliminar
F-PL-GST-01	Catálogo de Servicios de TI	SOP	2 años	5 años	7 años	Eliminar
G-PL-GSI-01	Medidas de Seguridad para Plataformas Digitales	SIN	2 años	5 años	7 años	Eliminar
GT-PL-ABD-01	Manual de Buenas Prácticas de Bases de Datos.	AAB	2 años	5 años	7 años	Eliminar
F-PL-ABD-01	Formato de Solicitud de Usuario Base de Datos	AAB	2 años	5 años	7 años	Eliminar

VII. CONTROL DE CAMBIOS

Fecha	Número de revisión	Actividad
31/01/2025	00	Generación del documento de Política para Gestionar la Seguridad Informática

VIII. FIRMA DE AUTORIZACIÓN DEL DOCUMENTO

Autorizó

Ing. Andres Mora Chang
Director de Gestión Tecnológica

Modelo de Seguridad Informática del Gobierno del Estado

ÍNDICE

		Página
I.	ANTECEDENTES	3
II.	PROBLEMÁTICA	7
III.	MARCO DE REFERENCIA	7
IV.	ALCANCE	15
V.	DESARROLLO DEL MODELO	15
VI.	SITUACIONES NO CONTEMPLADAS	17

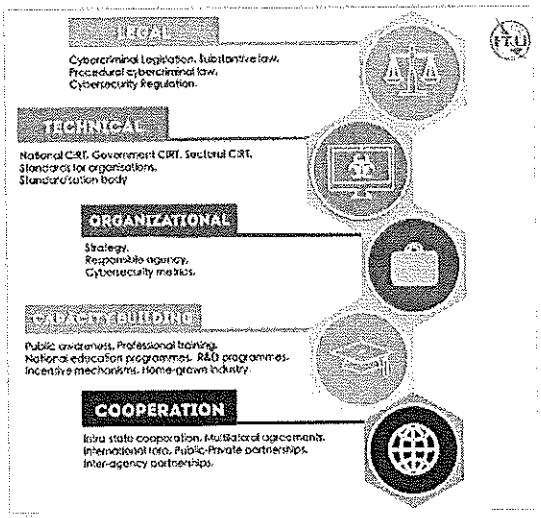
I. ANTECEDENTES

El Gobierno del Estado tiene como premisas garantizar los principios de igualdad de oportunidades para hombres, mujeres y personas en situación de vulnerabilidad, así como respetar y valorar el medio ambiente como condición indispensable para el desarrollo económico, político y social. Con el propósito de alcanzar estos fines, se elaboró el Plan Estatal de Desarrollo 2018-2024 (PED), que tiene como núcleo los derechos fundamentales de las personas.
Como parte de las líneas de acción establecidas en el PED, el Gobierno del Estado hace uso de la tecnología como habilitador de sus acciones, facilitando la realización de sus trámites y servicios acercándolos a la ciudadanía a través de plataformas tecnológicos mediante el uso de internet. Debido a esto, se debe considerar mayor enfoque a las medidas de seguridad debido a al incremento de manejo de información y transmitir confianza en la ciudadanía.
Esto conlleva a tener un mayor enfoque a las medidas de seguridad en la operación digital que el Gobierno del Estado debe implementar, tomando en cuenta mejores prácticas a nivel mundial en dicha materia.

La situación de la ciberseguridad, a nivel mundial.

En abril de 2015, la Unión Internacional en Telecomunicaciones (con siglas en inglés ITU), con la contribución del equipo ABI Research, establece el proyecto del Índice Global de Ciberseguridad (GCI), cuyo compromiso es el de ofrecer una instantánea de la situación en cuanto a la Ciberseguridad a Nivel Mundial, este compromiso es un resultados del compendio de las investigaciones sobre leyes, reglamentos, CERT y CIRT, políticas, estrategias nacionales, normas, certificaciones, formación profesional, sensibilización y asociaciones de colaboración. La idea era, fomentar la sensibilidad sobre ciberseguridad y el papel del gobierno, con la integración de los mecanismos para apoyar y promover esta disciplina. La salvaguarda de la integridad del ciberespacio, que conlleve el desarrollo de la ciberseguridad.

Los cinco pilares del Índice Global de Ciberseguridad (GCI), que monitorean el compromiso con la ciberseguridad en la cual, México es evaluado y toma posiciones en el ranking mundial, se contemplan a continuación:



Modelo de referencia (GCI, ITU 2018, P.5).

- **Legales**: las medidas se basan en la existencia de instituciones y marcos legales que tratan con temas de ciberseguridad y crimen cibernético.
- **Técnico**: las medidas se basan en la existencia de instituciones y marcos técnicos que se encargan de la ciberseguridad.
- **Organizacional**: las medidas se basan en la existencia de instituciones de coordinación de políticas y estrategias para el desarrollo de ciberseguridad a nivel nacional.
- **Capacidad**: las medidas se basan en la existencia de programas de investigación y desarrollo, programas de educación y capacitación, profesionales certificados y agencias del sector público que fomentan el desarrollo de las capacidades.

- **Cooperación**: las medidas se basan en la existencia de asociaciones, marcos de cooperación y redes de intercambio de información. (GCI 2019, P. 9).

El GCI para aplicar las posiciones regionales y globales, evalúa los cinco pilares mencionados y otorga a cada pilar un valor máximo de la unidad uno; así, todas las evaluaciones que otorguen de valor uno, se posicionan en el primer lugar. En México, en el 2018 fue evaluado con un índice general de 0.629 ocupando la posición número 63 de manera general y la posición 4 de manera regional muy por debajo de USA, Canadá y Uruguay como se muestra en la tabla del Ranking Global de América-2018.

Americas region

Member State	Score	Regional Rank	Global Rank
United States of America*	0.926	1	2
Canada*	0.892	2	9
Uruguay	0.681	3	51
México	0.629	4	63
Paraguay	0.603	5	66
Brasil	0.577	6	70
Colombia	0.565	7	73
Cuba	0.481	8	81
Chile	0.479	9	83
Dominican Republic	0.430	10	92
Jamaica	0.407	11	93
Argentina	0.407	11	94

Tabla del Ranking Global de América 2018 (GCI, ITU 2019, P.56).

La situación de la ciberseguridad en América Latina y el Caribe

La Organización de los Estados Americanos (siglas OEA), fue creada en 1948 cuando se suscribió en Bogotá Colombia, la Carta de la OEA, posteriormente fue enmendada por el protocolo de Washington suscrito en 1992; cuyo objetivo es lograr que los 35 Estados miembros hoy en día, contribuyan al foro gubernamental político, jurídico y social de este hemisferio y como lo estipula el Artículo 1 de la Carta "un orden de paz y de justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial y su independencia".

En el 2013, en un estudio realizado en colaboración con la Organización de los Estados Americanos, Symantec, AMERIPOL, Anti-Phishing Working Group (APWG), LACNIC, Microsoft e ICANN; presentaron un informe del panorama general en materia de seguridad y delitos cibernéticos que tuvieron lugar en América Latina y el Caribe. Estas tendencias globales, fueron el ciber espionaje (en materia de privacidad) y las violaciones a la seguridad con fines financieros (la infiltración a empresas y gobierno, para lograr acceso a información confidencial).

La situación en México y en el Estado de Yucatán

El gobierno federal mexicano publicó en el 2017 un documento de intención para coordinar esfuerzos en materia de ciberseguridad, La Estrategia Nacional de Ciberseguridad (ENCS) es el documento que establece la visión del Estado mexicano en la materia, a partir del reconocimiento de:

- La importancia de las tecnologías de la información y comunicación (TIC) como un factor de desarrollo político, social y económico de México; en el entendido de que cada vez más individuos están conectados a Internet y que tanto organizaciones privadas como públicas desarrollan sus actividades en el ciberespacio.
- Los riesgos asociados al uso de las tecnologías y el creciente número de ciberdelitos.
- La necesidad de una cultura general de ciberseguridad.

Aunque la estrategia no fue coordinada exitosamente, establece criterios de intención positiva, en el resumen de acciones y objetivo general:

Para cumplir con el objetivo general, se establecen 5 objetivos estratégicos:

1. Sociedad y derechos.
2. Economía e innovación.
3. Instituciones públicas.
4. Seguridad pública.
5. Seguridad nacional.

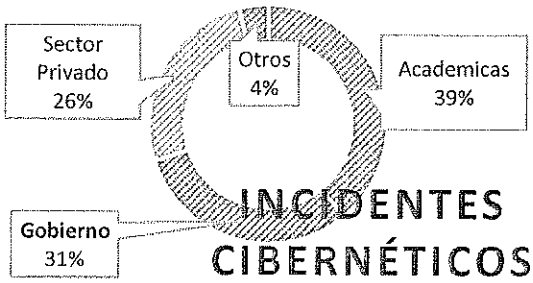
Para el desarrollo de la ENCS, se consideran tres principios rectores:

A. Perspectiva de derechos humanos.
B. Enfoque basado en gestión de riesgos.
C. Colaboración multidisciplinaria y de múltiples actores.

Para alcanzar los objetivos estratégicos, se desarrollan 8 ejes transversales:

1. Cultura de ciberseguridad.
2. Desarrollo de capacidades.
3. Coordinación y colaboración.
4. Investigación, desarrollo e innovación TIC.
5. Estándares y criterios técnicos.
6. Infraestructuras críticas.
7. Marco jurídico y autorregulación.
8. Medición y seguimiento." (Gobierno de México 2017, P.4).

Dentro del contexto contemporáneo, los históricos del 2013, de los incidentes cibernéticos denunciados en la cual, prevaleció el 39% contra Organizaciones Académicas, el 31% contra Instituciones Gubernamentales, el 26% contra Entidades del Sector Privado y el 4 % contra otros; fueron principalmente, sobre las estafas en los medios sociales, los códigos maliciosos, para los dispositivos móviles; el ransomware y otras conductas delictivas, que utilizaban medios electrónicos. (OEA 2014, P.67).



Incidentes cibernéticos, Información, OEA 2014, P.67; Elaboración, Departamento de Seguridad Informática

La Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI), en colaboración con la Asociación Mexicana de Tecnologías de la Información (AMITI) y la Asociación de Internet MX, presentaron los resultados del estudio "Evaluación de la Ciberseguridad en México: Brechas y Recomendaciones en un Mundo Hiper-Conectado"; destacando la necesidad de contar con una Agencia Nacional de Ciberseguridad Nacional, la importancia de redefinir el marco jurídico para la ciberseguridad, garantizar la protección de infraestructura crítica y el desarrollo de habilidades, reclutando el mejor talento posible.

Las brechas más importantes de las organizaciones mexicanas fueron, en cuanto a la clasificación de información, métricas de ciberseguridad, capacitación en continuidad de negocio y pruebas de vulnerabilidades por terceros. Destacando que solo el 65.3% de las organizaciones participantes se consideran medianamente preparadas para hacer frente a las amenazas (CANIETI).

Desde el 2017, la coordinación de la Unidad Especializada en Delitos Cibernética de la Fiscalía General del Estado de Yucatán, con el objeto de apoyar en la investigación de los hechos presuntamente delictivos que se cometan por medios informáticos; mantiene un histórico de delitos cibernéticos de acuerdo a las solicitudes de investigación realizadas por la misma; atendiendo delitos contra la suplantación de identidad, acoso y/o difamación cibernética, robo de información y delitos financieros; por mencionar algunos.

Recientemente, con la aprobación y modificación al Código Penal del Estado de Yucatán, en materia de Delitos informáticos se apertura un gran esfuerzo contra quienes provoquen la pérdida de información contenida en sistemas o equipos electrónicos protegidos por algún mecanismo de seguridad. Además, se añadió también las sanciones para quienes faciliten a un tercero, o ayuden a sustraer información privada o confidencial. (Poder Legislativo del Estado de Yucatán, 2019).

Resultan claras dos grandes vertientes acerca de la implementación de una postura de ciberseguridad en una organización, la primera es que la práctica de realizar los inventarios de activos digitales, y los procesos clave que interactúan con esos activos, permite a la organización identificar plenamente los núcleos sustantivos que permiten la operación y que aportan valor a la organización, la reiteración de auditar y generar controles sobre estos activos, permiten la mejora continua sobre las piedras angulares que sostienen la operación de una organización. La segunda es la clara tendencia acerca de la ventaja competitiva, de posicionamiento o calificación positiva sobre los procesos de

la organización, incluso organizaciones a nivel gobierno, se han vuelto punto de referencia por su ventaja de administración gubernamental, apoyados fuertemente por un entorno de transformación digital con acompañamiento de prácticas sólidas de ciberseguridad.

II. PROBLEMÁTICA

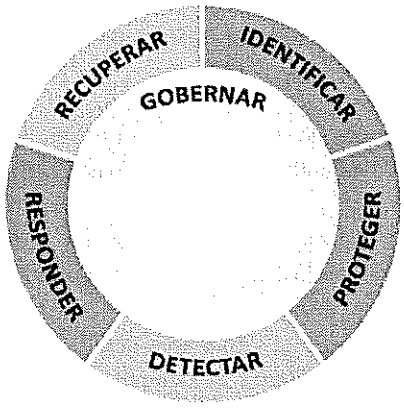
El aumento de manejo de información y la realización de acciones por vías digitales conlleva a incrementar las medidas de seguridad informática, debido a los riesgos y vulnerabilidades a los que los Activos Digitales y Componentes Tecnológicos involucrados en la operación se encuentran expuestos. Estos riesgos y vulnerabilidades pudieran generar perdida de datos, filtración de información, ciberataques a servicios públicos, robo de identidad y otras posibles consecuencias.

El Gobierno del Estado, requiere fortalecer las directrices para homologar los criterios y estrategias relacionadas con la seguridad informática. A partir de esto, las Dependencias y Entidades deban realizar las acciones requeridas para procurar la seguridad de los Habilitadores Tecnológicos involucrados en su operación.

III. MARCOS DE REFERENCIA.

Basado en las recomendaciones acerca de mejores prácticas y estándares internacionales de seguridad informática, se puede tomar como base un modelo que pueda implementarse como estrategia a seguir en la implementación de prácticas de reforzamiento de ciberseguridad, además de cumplir con condiciones que favorezcan su adopción, como:

- Patrocinadores e interesados ejecutivos, totalmente dispuestos.
- Jerarquía o autoridad del departamento gestor, responsable del seguimiento de implementación.
- Presupuesto suficiente.
- Personal suficiente, para realizar las mejoras en paralelo sin afectar la operación.
- Auditores entrenados en el modelo a implementar.
- Responsables técnicos con conocimiento del modelo a implementar.
- Procesos y procedimientos documentados.



Tomando como base el marco de referencia NIST 2.0, las 6 grandes categorías que engloban las herramientas que se pueden generar para crear un reforzamiento desde el punto de vista de la ciberseguridad son los siguientes:

Gobernar: Desarrollar e implementar estrategias, expectativas y la política de gestión de riesgos de seguridad cibernética de la organización, además de establecer medios que comuniquen y supervisen estratégicamente dichas medidas.

Identificar: Desarrollar un entendimiento organizacional, para administrar los riesgos de ciberseguridad hacia los sistemas, activos, datos y capacidades.

Proteger: Desarrollar e implementar medidas para la gestión de riesgos y las salvaguardas apropiadas para asegurar los activos y la entrega de servicios de la organización.

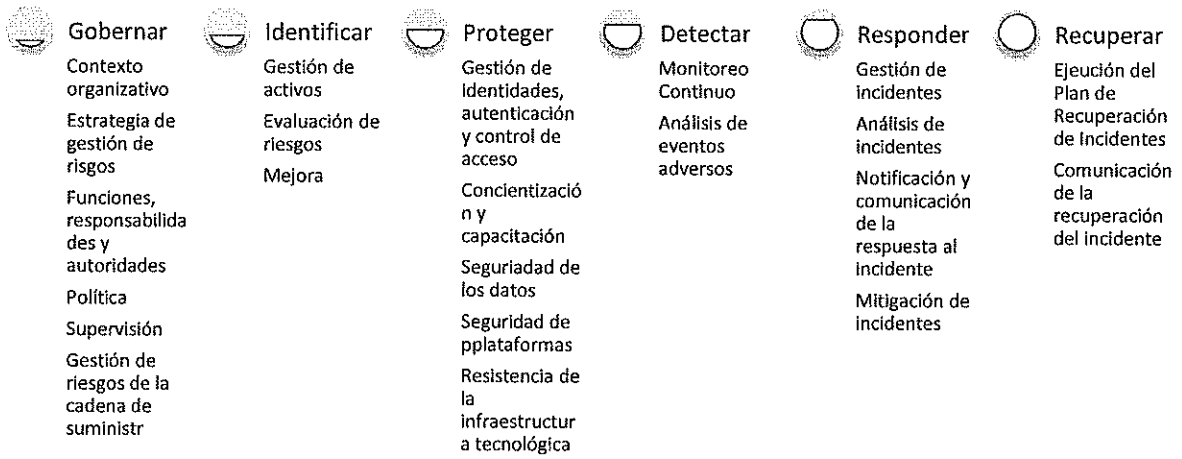
Detectar: Desarrollar e implementar actividades apropiadas para identificar y analizar la ocurrencia de un evento de ciberseguridad.

Responder: Desarrollar e implementar las actividades apropiadas para tomar acciones al respecto, una vez detectado un incidente de ciberseguridad.

Recuperarse: Desarrollar e implementar actividades apropiadas para la recuperación de los activos y las operaciones afectadas que haya sido mermado como consecuencia de un incidente de seguridad o un procedimiento de respuesta, así como mantener planes para la resiliencia.

Estructura Conceptual para la Implementación de Herramientas.

El valor que puede aportar la implementación de una u otra herramienta para la atención de las etapas mencionadas, será en la medida que ésta aporte benéficamente en la administración, protección, reforzamiento y resiliencia en caso de falla, en un determinado proceso, servicio o información. Cada una de estas herramientas toma protagonismo en diferentes categorías y en diferentes momentos.



Algunas de las herramientas individuales que pueden usarse en el marco de referencia NIST se presentan a continuación:

- ***Accesos remotos seguros***, permite establecer canales seguros de comunicación, a través de los cuales, la información se puede transmitir por redes no seguras o no confiables; incluidas como no confiables, las redes públicas de Internet.
- ***Administración de credenciales***, permite almacenar y realizar de forma segura las actividades de la administración de las credenciales, como los cambios de contraseña, el cambio y/o asignación de los niveles de privilegios, entre otros.
- ***Administración de incidentes***, permite documentar, dar seguimiento y coordinar la mitigación de un evento adverso en los dispositivos informáticos y de red del sistema. Minimiza los tiempos de inactividad debido a incidentes adversos y aumenta la eficiencia y productividad del sistema.
- ***Administración de interfaz de red,*** permite controlar las conexiones y la estadística de la información recibida y transmitida, a través de los puertos físicos en los dispositivos de red.
- ***Administración de la configuración***, permite establecer y mantener la integridad de los sistemas que controlan los componentes de hardware y software, en el proceso de tener que llevar un control para iniciar, cambiar, monitorear y auditar la configuración de los componentes a través del ciclo de desarrollo del sistema.

La administración de la configuración, ayuda a garantizar que los sistemas se desarrollen en un estado consistentemente seguro para mantenerlos a lo largo de su vida útil. Reduciendo el riesgo de interrupciones, debido a problemas de configuración y violaciones de seguridad a través de una mejor visibilidad y seguimientos en los cambios en el sistema.

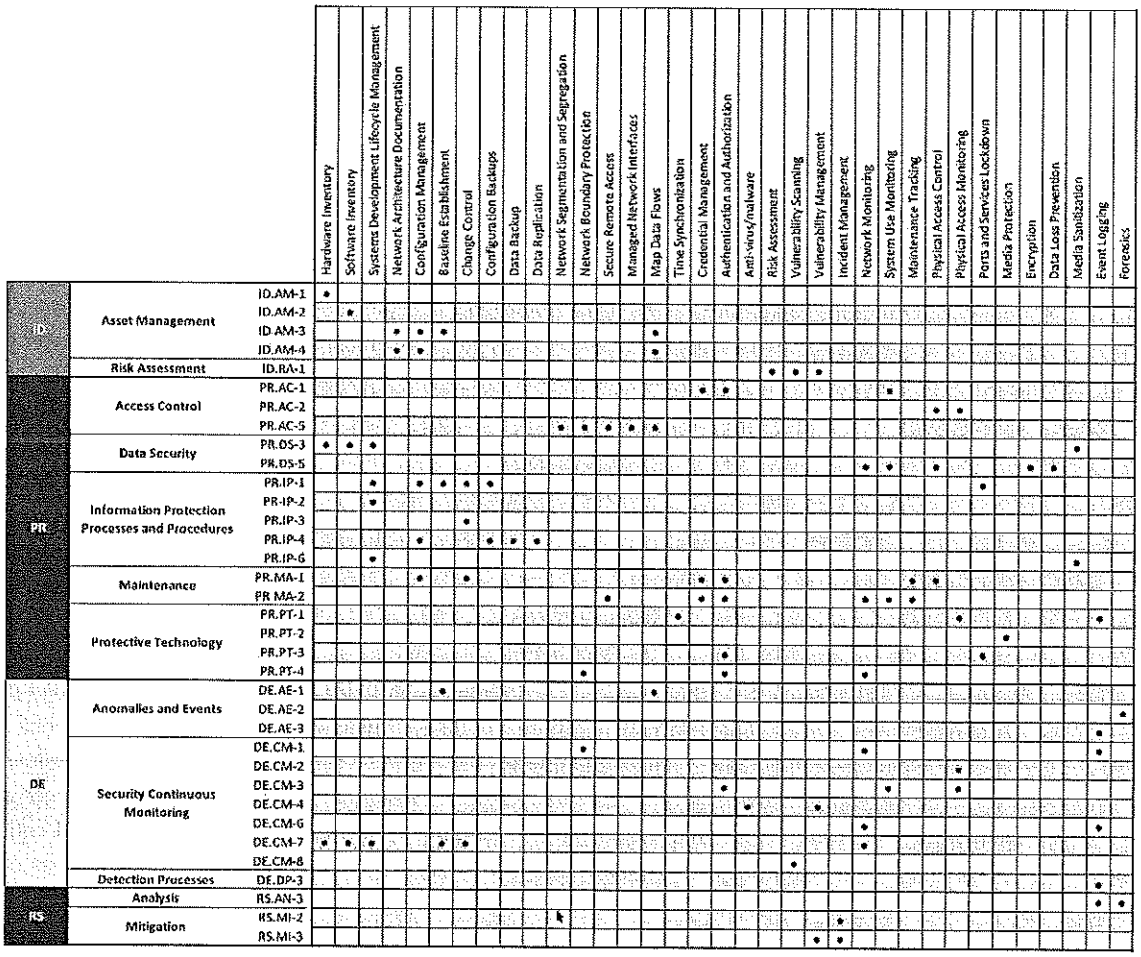
- ***Administración de vulnerabilidades***, permite documentar, administrar y mitigar las vulnerabilidades detectadas en el sistema. También permite aplicar las actualizaciones de seguridad al sistema e identificar dónde se necesitan controles compensatorios, para proteger los dispositivos informáticos que no puedan ser actualizados.
- ***Administración del ciclo de vida del desarrollo del sistema,*** permite rastrear el alcance de las actividades asociadas con los componentes de hardware y software del sistema, contempla el inicio, desarrollo, adquisición, implementación, operación y mantenimiento de cada componente y por último, el desmantelamiento.
- ***Administración del riesgo,*** es un documento estratégico que define el cómo se identificarán, analizarán y administrarán los riesgos asociados con la organización. Describe la estrategia de la administración del riesgo para la organización; además, proporciona la terminología, el estándar, las funciones y responsabilidades, entre otros detalles del proceso de la administración del riesgo. Este documento, puede ser utilizado para comprender los riesgos, estimar los impactos y definir la respuesta al problema y está diseñado para guiar al equipo del proyecto y a las partes interesadas (responsables, dueños de procesos, etc.).
- ***Antivirus/antimalware,*** permite supervisar a los dispositivos informáticos para identificar los principales tipos de programas maliciosos (malwares) existentes y de esta manera prevenir o contener el incidente. Los programas o códigos maliciosos, son las amenazas más comunes y el antivirus debe proteger a los dispositivos informáticos, de ser infectados con ransomware, virus, gusanos, troyanos, entre otros.
- ***Arquitectura de la red,*** permite identificar, documentar y diagramar las interconexiones entre los dispositivos conectados en red del sistema, las redes corporativas y otras conexiones externas. Documentar detalles del entorno de los dispositivos de la red y las interconexiones, es la pieza clave. Además, comprender las interconexiones dentro del entorno, es crítico para el éxito del desarrollo de los controles de ciberseguridad. Esta información, es también importante, para el monitoreo efectivo.
- ***Autenticación y autorización***, esta herramienta permite al gestor, verificar la identidad del usuario y aplicar los principios del mínimo de privilegios. Esta herramienta, permite determinar los permisos en los usuarios para acceder a un recurso del sistema.
- ***Bloqueo de puertos y servicios***, las soluciones de este tipo, permiten a fabricantes realizar la detección y la facilidad de deshabilitar los puertos y servicios no esenciales de red, físicos y lógicos.
- ***Cifrado,*** permite la protección los datos confidenciales de un sistema, de modo que solamente los usuarios autorizados puedan descifrarlos y acceder a ellos.
- ***Control de cambios***, permite documentar, dar seguimiento y coordinar cambios a los componentes de hardware y software del sistema. Muchas interrupciones pueden ser prevenidas con configuraciones efectivas y programas de control de cambios. Un proceso de control de cambios asegura que los cambios son documentados y revisados por personal apropiado y se aprueba el cambio.
- ***Controles de acceso físicos***, esta solución permite limitar el acceso físico solo a personas autorizadas, para proteger el sistema de personas malintencionadas, previniendo de daños accidentales o no intencionales, a componentes críticos.
- ***Escaneo de vulnerabilidades***, permite escanear, detectar e identificar defectos de software o configuraciones erróneas, que causan una debilidad en la seguridad del sistema. La identificación de vulnerabilidades

conocidas de seguridad, se pueden utilizar para ayudar e informar durante las actividades de administración de vulnerabilidades.

- ***Establecer línea base***, permite el soporte de la administración de la configuración de los sistemas o recursos configurables. El uso de línea base, es uno de los métodos usados para implementar la administración de la configuración de una manera automática.
- ***Evaluación de riesgos***, esta herramienta permite realizar la evaluación del riesgo a los sistemas de la organización. Al realizar la evaluación del riesgo, se identifican las vulnerabilidades de seguridad actuales, se controlan las brechas de seguridad y el incumplimiento de las normas. Se realizan a través de auditorías que consisten en encuestas, cuestionarios, entre otros. Esta forma parte, de un proceso de administración del riesgo, proporcionando a las partes interesadas la información necesaria, para determinar los cursos de acción apropiados en respuesta a los riesgos identificados.
- ***Forense (análisis),*** permite identificar, recopilar, examinar y analizar los datos de los sistemas para determinar la causa raíz de un incidente. La recopilación de los datos relacionados con la ciencia forense dentro de un entorno de red, proporciona la capacidad de examinar los datos en busca de pruebas necesarias, para determinar las actividades malintencionadas e identificar al actor responsable.
- ***Inventario de hardware,*** permite el seguimiento de los dispositivos de cómputo y de red dentro del sistema de información, incluyendo detalles de dispositivos e información de localización.
- ***Inventario de software y firmware***, permite el seguimiento de software y firmware instalado dentro del sistema de información en computadoras y dispositivos de red, incluyendo identificación, versión de software e información de localización, entre otros.
- ***Mapa de flujo de datos***, esta herramienta permite comprender y documentar el flujo del dato entre los componentes de la red y el sistema; siendo de ayuda principalmente, a la resolución de problemas, en las actividades de respuesta, recuperación y para el análisis e identificación de anomalías.
- ***Monitoreo de acceso físico***, permite supervisar, archivar y auditar el acceso físico al sistema para todas las personas. La capacidad de registrar, supervisar, archivar y auditar el acceso físico a la instalación y ubicación proporciona visibilidad de la presencia física de las personas.
- ***Monitoreo de la Red,*** permite recabar, almacenar y auditar el tráfico de la red del sistema. Además, monitorear los indicadores de posibles incidentes de ciberseguridad, pudiendo identificar el tráfico sospechoso y otros vectores de amenaza, lo que permite responder a un incidente.
- ***Monitoreo del uso del sistema,*** permite supervisar el uso del sistema, permitiendo almacenar, auditar y restringir las actividades de los usuarios del sistema.
- ***Operaciones de ciberseguridad***, es un documento que define los pasos operativos que los administradores y demás empleados, deberán seguir para garantizar la coherencia con la respuesta a los eventos que ocurren dentro del sistema.
- ***Plan de recuperación del sistema***, es un documento diseñado para garantizar la continuidad de los procesos críticos o vitales de la organización, en caso de que ocurriera un incidente de ciberseguridad. Su propósito es, proporcionar un enfoque estructurado para responder al incidente de ciberseguridad, aprovechando el inventario de infraestructura y la información de configuración relevante para restaurar las capacidades operativas. El plan debe ir desarrollado con los siguientes objetivos, evaluar y reparar el daño, restaurando el sistema. Administrar la operación de recuperación de manera organizada y efectiva, preparando al personal para responder en situaciones de recuperación del sistema. Limitar la magnitud de cualquier pérdida, al minimizar la duración de la interrupción.
- ***Plan de respuesta a incidentes***, es un documento que describe el plan para responder a incidentes de seguridad de la información dentro de la organización. Define los roles y responsabilidades de los participantes, las

características o tipos de incidentes, las relaciones con otras políticas y/o procedimientos y los requisitos del informe. El objetivo de un plan de respuesta a incidentes cibernéticos es detectar y reaccionar ante el incidente, comunicar los resultados y el riesgo a las partes interesadas y evitar o reducir la probabilidad de que el incidente vuelva a ocurrir.

- ***Política de ciberseguridad***, es un documento que define los requisitos de ciberseguridad para el uso adecuado y seguro de los servicios de Tecnología de la Información en la organización. Su objetivo es proteger a la organización y a sus usuarios, en la medida de lo posible contra las amenazas de ciberseguridad que podrían poner en peligro su integridad, privacidad, reputación y los resultados organizacionales.
- ***Prevención de pérdida de datos***, esta herramienta permite prevenir la pérdida de la información o dato, detectando y evitando el acceso no autorizado y la transmisión de datos confidenciales del sistema.
- ***Programa de ciberseguridad***, es un documento que establece los principios para iniciar, implementar, mantener y mejorar la administración de la ciberseguridad; apoyado de un conjunto de documentos como las políticas, los procedimientos, los estándares y/o las guías, de ciberseguridad, entre otros. Este programa, debe estar diseñado para proteger la confidencialidad, integridad y disponibilidad de los recursos de información.
- ***Protección de los límites en la red,*** esta solución permite al gestor controlar el tráfico de comunicación de datos desde y hacia las redes del sistema. Las capacidades de protección del límite de la red, incluyen, el uso de firewalls, zonas desmilitarizadas (DMZ), sistemas de detección y prevención de intrusos, entre otros.
- ***Protección del medio***, esta solución permite restringir el uso de medios portátiles en el sistema.
- ***Registro de eventos,*** permite capturar, almacenar, archivar y auditar los eventos que se producen en el sistema y las redes. Esta herramienta, proporciona información importante sobre las operaciones del sistema, ayudando significativamente a prevenir las brechas e incidentes de seguridad.
- ***Replicación de datos,*** permite copiar y transferir respaldos de seguridad de datos a una localización física externa para el sistema. Se debe proporcionar la separación física, que garantice la integridad de los datos. Además, puede ser acompañada con herramientas de encriptación que son usadas en ambos hardware y software, para garantizar a la organización que sus datos estén a salvo de accesos no autorizados.
- ***Respaldo de configuración***, permite recopilar y archivar los ajustes de configuración de los componentes de hardware y software del sistema, en un formato de datos especificado por el fabricante del equipo original (OEM). La copia de seguridad de la configuración de un dispositivo, permitirá la restauración operativa del dispositivo a un punto específico en el tiempo, cuando se produce un incidente.
- ***Respaldo de datos,*** permite recolectar y almacenar archivos, programas del sistema y demás para facilitar la recuperación después de un incidente. La copia de seguridad de los datos, permite restaurar los datos a un punto específico en el tiempo, recuperándose de un incidente.
- ***Sanitización del medio***, permite renderizar los datos escritos en un medio, de modo que resulten irrecuperables.
- ***Segmentación y segregación de la red***, esta solución permite separar las redes de sistema de otras redes, segmentar el sistema interno dentro de redes pequeñas y controlar la comunicación entre específicos host y servicios.
- ***Seguimiento del mantenimiento***, permite realizar un seguimiento, programar, autorizar, auditar las actividades de mantenimiento y reparación de los dispositivos informáticos del sistema.
- ***Sincronización del tiempo,*** esta solución permite sincronizar el tiempo que registran en los equipos, para que todos los componentes del sistema generen marcas de tiempo precisas.



Matriz de herramientas de seguridad. NIST

IV. ALCANCE

La Subsecretaría de Tecnologías de la Información y Comunicaciones, tomando como referencia las etapas establecidas por el marco de referencia NIST y como ente encargado de establecer las directrices en la operación tecnológica del Gobierno del Estado, define un modelo que contempla la implementación de acciones en las etapas: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar, integradas en la normativa:

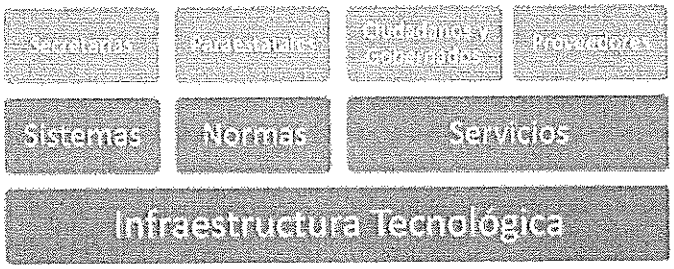
- PL-STI-11 Política para Gestionar la Seguridad Informática
- G-PL-GSI-01 Medidas de Seguridad para Plataformas Digitales

Cabe mencionar que lo anterior son marcos de referencia para que las Dependencias y Entidades, de acuerdo al contexto y posibilidades de infraestructura y recursos para su implementación, adopten las acciones y herramientas que mejor se alineen a este modelo.

V. DESARROLLO DEL MODELO

El modelo de implementación, puede constar de prácticas internas correctamente documentadas, apego parcial o total a marcos de referencia, considerando en todo momento la obligación legal y el cumplimiento de normas. La Subsecretaría de Tecnologías de la información, tiene la responsabilidad de emitir hacia las dependencias y secretarías, normas y requisitos a cumplir en materia de tecnologías, y la ciberseguridad debe considerarse dentro de estas normas.

La aplicación consistente y homologada de criterios de normatividad hacia toda la organización, empodera a la misma en la consecución de sus objetivos, empoderados por las tendencias de transformación digital. Al efectuar las actividades para la generación de normatividad en los procesos sustantivos de la subsecretaría, al ser éstos de aplicación global, por consecuencia directa se afectarán a los procesos de las dependencias que hagan uso de los elementos auditados y normados.



Dependencia de los Sistemas de Información

El reforzamiento de las prácticas de seguridad informática permite asegurar la mejora continua en múltiples aspectos colaterales deseables:

- **Transparencia**. Los controles, inventarios y registros permiten auditar sucesos, eventos y permite el seguimiento en la evolución de un suceso relevante.
- **Transiciones continuas**. La documentación precisa de los componentes, el entrenamiento continuo y los procedimientos normados permiten la transición de empleados, servicios, sistemas e incluso administraciones con un alto grado de confiabilidad y corta curva de aprendizaje.
- **Servicios digitales de vanguardia**. Conocer las capacidades tecnológicas de la organización permite identificar debilidades o límites a resolver en la implementación de nuevas y mejores tecnologías a un ritmo más avanzado, pues acorta el tiempo de entendimiento de los componentes al momento de revisar cumplimientos de requerimientos mínimos y capacidades. Permite incluso trazar rutas de mejora por etapas.

Las organizaciones que han habilitado practicas efectivas de ciberseguridad, han podido mejorar sus indicadores en materia de:

- Disminución en eventos de interrupción de operaciones.
- Disminución en tiempos fuera de operación por incidentes.

- Administración de bienes con menor porcentaje de merma.
- Ahorros por anticipación de compras en tecnología, por análisis de inventario y obsolescencia.
- Gobernanza efectiva en incidentes y administración de tecnología.
- Aumento en la confianza y aceptación de la organización dentro del mercado meta o población objetivo.

La implementación de las herramientas, deben de complementarse con la adopción de una estrategia a seguir, un eje transversal de implementación como objetivo paralelo de cumplimiento organizacional, como pueden ser:

- Fomentar acciones que resulten en el incremento de una cultura de ciberseguridad.
- Crear oportunidades que permitan el desarrollo de capacidades de los empleados y responsables.
- Establecer canales que permitan la coordinación y colaboración de los profesionales de TI.
- Fomentar la investigación, el desarrollo y la innovación en materia de TI.

Metodología.
La metodología que aplicará para la implementación de las herramientas que permitan habilitar las prácticas de ciberseguridad en la organización, deberán seguir las siguientes consideraciones.

- Identificación de los activos de información.
- Clasificación de los activos de información, con respecto a la legalidad de esta.
- Clasificación de los activos de información, con respecto al valor que les sea otorgado.
- Documentación del impacto por la pérdida o daño a esos activos de información.
- Enlistar y priorizar las actividades que mitiguen el riesgo hacia esos activos de información.
- Programar revisiones y modificaciones.

Estas actividades llevarán a la selección de las herramientas a implementar. El proceso de mejora continua permitirá ir agregando los controles complementarios gradualmente e implementar paulatinamente nuevas herramientas.
En términos generales, se debe Identificar la información de valor, clasificarla, realizar el análisis de riesgos hacia esa información, acordar el nivel de aceptación, mitigación o tercerización del riesgo, establecer planes de continuidad, monitorear el cumplimiento y programar mejoras, todo en un ciclo continuo de evolución sistemática.

Despliegue de Acciones.
Como punto de partida para el desarrollo de las acciones relacionadas con la seguridad informática las Dependencias y Entidades deben llevar controles que identifiquen el estado actual en que se encuentran y las acciones que consideren de mejora y un monitoreo del avance proyectado.

VI. SITUACIONES NO CONTEMPLADAS

Cualquier situación, cambio, actualización o excepción referente a este modelo, se gestionará, aprobará y comunicará a través de las entidades pertinentes del Gobierno de Tecnologías.

RENACIMIENTO MAYA YUCATÁN GOBIERNO DEL ESTADO · 2024 · 2030	**SECRETARÍA DE ADMINISTRACIÓN Y FINANZAS** Subsecretaría de Tecnologías de la Información y Comunicaciones	YUCATAN

Formato de Solicitud de Usuario de Base de Datos

DATOS DEL USUARIO SOLICITANTE					
Nombre Completo:				**Fecha de Solicitud:**	Elija una fecha
Jefe inmediato:		**Empresa /dirección:**		**Área:**	
Teléfono:		**Ext:**		**Correo:**	
Folio del cambio:	[# Ticket]		**Usuario:**	☐Interno ☐Externo	
Requerimiento:	☐Alta Usuario ☐ Actualización Permisos ☐Baja Usuario ☐Renovación de cuenta				

CUENTA DE BASE DE DATOS SOLICITADA			
Login:		**Tipo de usuario:**	☐Base de Datos ☐ Aplicación

DETALLES DEL ACCESO			
Nombre de la Base de Datos:		**Plataforma:**	Elegir un elemento
Instancia:		**Puerto de Base de Datos:**	
Servidor:	[Nombre del servidor]	**IP Servidor:**	[192.168.X.X]
Tipo de Base de datos	☐QA ☐Desarrollo ☐ Producción ☐ Pre-Producción	**Caducidad de la contraseña:**	☐ 30 días para internos y Externos ☐180 Días para internos y Externos ☐ Permanente para Aplicación
Se otorga privilegios a:	☐Usuario ☐ Grupo ☐ Rol	**Caducidad del Login:**	☐Permanente para Aplicación ☐Permanente para Internos ☐90 Días para externos
Justificación del requerimiento:	[Describir cual es el motivo, que función tendrá el usuario, y para que se estará utilizando]		

EQUIPO DE DONDE SE REALIZARÁN LAS CONEXIONES A LA BASE DE DATOS			
Nombre del equipo 1:		**Dirección IP:**	
Nombre del equipo 2:		**Dirección IP:**	
Nombre del equipo 3:		**Dirección IP:**	

OBJETOS A LOS QUE SOLICITA EL ACCESO							
Objeto de base de datos (Tabla, SP, Vista, Fn)	**Nombre Objeto**	**PERMISOS** (Escribir la letra X para asignar los permisos correspondientes)					
		UPDATE	**SELECT**	**INSERT**	**DELETE**	**EXECUTE**	**OTROS**

OTROS:	[Describir que tipo de permiso se requiere]
PARA EL USO DEL DBA	
Observaciones del DBA:	

PARA USO DEL ÁREA DE BASE DE DATOS			
Dueño o Responsable de la base de datos:		**Firma y fecha de conformidad:**	Haga clic aquí o pulse para escribir una fecha.
Nombre del Gerente y/o Director que Autoriza la solicitud:		**Firma y fecha de conformidad:**	Haga clic aquí o pulse para escribir una fecha.

OBSERVACIONES DEL DUEÑO O RESPONSABLE DE LA BASE DE DATOS	
Observaciones:	

RESPONSABLE DE BASE DE DATOS QUE APLICA LA SOLICITUD			
Nombre Completo del DBA:		**Firma y fecha de conformidad:**	Haga clic aquí o pulse para escribir una fecha.

Catálogo de Servicios de TI

ID	Servicios	Tipo	SLA	Pre requisitos	Lista de Cotejo	Normativa Relacionada

Gobierno del Estado de Yucatán

Secretaría de Administración y Finanzas

Manual de Buenas Prácticas de Bases de Datos

Índice

I. Objetivo 3

II. Alcance 3

III. Estándares generales de buenas prácticas de base de datos 3

1. Estándares de Creación de Base de Datos 3

1.1. Nombre de Usuario y Contraseña 3

1.2. Configuraciones del motor de base de datos 4

1.3. Objetos de base de datos 4

1.4. Gestión Documental 8

1.5. Scripts de base de datos 9

1.6. Transaccionalidad 11

1.7. Respaldos de base de datos 11

1.8. Mantenimientos de Bases de Datos 12

1.9. Monitoreo de las Bases de Datos 13

1.9.1. Comportamiento de la base de datos: 13

1.9.2. Crecimiento de las áreas de datos. 13

1.9.3. Estadística de base de datos 13

1.10. Nivel de Criticidad de los Servicios Especializado de Bases de Datos 13

I. Objetivo

Definir las estrategias y lineamientos a seguir para la creación y gestión de proyectos, logrando un mejor desarrollo de aplicaciones en plataforma MySQL, PostgreSQL, SQL Server o Progress OpenEdge, administradas por el área de Administración de Base de Datos. Con el objetivo de incentivar a analistas y desarrolladores aplicar un enfoque orientado a la optimización de los aplicativos del Gobierno del estado de Yucatán a través del uso de estándares y buenas prácticas.

II. Alcance

Este documento sólo aplica a las entidades y áreas que corresponden al Gobierno del Estado de Yucatán.

III. Estándares generales de buenas prácticas de base de datos

1. Estándares de Creación de Base de Datos

1.1. Nombre de Usuario y Contraseña

1.1.1. La nomenclatura para la creación de usuarios de base de datos, se divide en dos, usuario de aplicación y usuario de base de datos, para el usuario de aplicación deberá de iniciar con la nomenclatura "usrsistema_", seguido del nombre del sistema, para los usuarios de base de datos se deberá crear como se encuentra en el Active Directory.

Ejemplo de usuario de aplicación:

```
usrsistema_contable
```

Ejemplo de usuario de base de datos:

```
maria.perezj
```

1.1.2. Cada sistema gestor de base de datos tiene sus propias recomendaciones y limitaciones para el nombre de usuario y contraseña.

a) MySQL: Los nombres de usuario y contraseñas en MySQL pueden tener como máximo 16 caracteres de longitud. Las contraseñas deben cumplir con los siguientes requisitos: Al menos 10 caracteres de longitud, 1 mayúscula, 1 minúscula, 1 número y 1 carácter especial.

Ejemplo:

```
CREATE USER 'usuariodeprueba'@'localhost' IDENTIFIED BY 'Passw32!';
```

b) PostgreSQL: La longitud máxima permitida para el nombre de usuario y la contraseña es de 63 caracteres. Se recomienda que la contraseña contenga al menos 10 caracteres, 2 mayúsculas, 2 minúsculas, 2 números y 2 caracteres especiales.

Ejemplo:

```
CREATE USER nombreusuario PASSWORD 'ContraSeña13?!';
```

c) Progress: El nombre de usuario puede ser una cadena de hasta 32 caracteres y deben comenzar con un carácter de a-z o de A-Z. El nombre de usuario puede consistir de caracteres alfabéticos, dígitos y los siguientes caracteres especiales: # $% & - _.

Las contraseñas definidas para los usuarios pueden ser una cadena de hasta 16 caracteres sensibles a mayúsculas y minúsculas. (Si escribe más de 16 caracteres en el campo Contraseña, no se aceptarán los caracteres adicionales). Las contraseñas no deben tener caracteres especiales.

Ejemplo:

```
CREATE USER 'Jasper', 'NuevaContrDbausr';
```

1.2. Configuraciones del motor de base de datos

1.2.1. Collation de base de datos: también conocido con "intercalación de base de datos", es un parámetro de la base de datos que se utiliza para configurar las reglas y caracteres del contenido apropiadamente según idioma o alfabeto en el que se encuentre, cada motor de base de datos cuenta con una configuración diferente, las cuales se indican a continuación:

a. MySQL Server: utf8_unicode_ci, como collation por defecto.
b. SQL Server: Modern_Spanish_CI_AS, como collation por defecto.
c. PostgreSQL Server: en_US.UTF-8, como collation por defecto.
d. Progress OE: American,United_State,ISO8859-1,Basic,Basic' , como collation por defecto.

1.2.2. La base de datos deberá ser normalizada en su tercera forma normal.

1.3. Objetos de base de datos

1.3.1. Las tablas deben tener siempre una llave primaria o identificador de la tabla, el cual puede ser un único campo de tipo INT IDENTITY o tipo UNIQUE IDENTIFIER, evitar tener nombres de clave primaria semánticamente significativos. Un error de diseño clásico es crear una tabla con clave principal que tenga un significado real como "nombre" como clave principal. En este caso, si alguien cambia su nombre, la relación con otra tabla se afectará y el nombre puede ser repetitivo (no único).

1.3.2. Utilizar minúsculas para nombrar a los diferentes objetos de base de datos como son tablas, vistas, columnas (incluyendo aquellas que formen parte de una llave), procedimientos almacenados y funciones de usuario.

Ejemplo:

vw_requisicion_compras / usp_saldoscuentas / fn_estatus_requisicion

1.3.3. Los nombres de las bases de datos no deben incluir abreviaturas, estos deberán ser cortos y concisos, y en caso de ser largos se deberá hacer uso de guiones bajos para separar las palabras.

Ejemplo incorrecto:

Rt-Noct-Trans

Ejemplo correcto:

RUTA_NOCTURNA_TRANSPORTE / ruta_nocturna_transporte

1.3.4. Para todo objeto de base de datos, se deberá de utilizar guiones bajos para separar nombres que contengan más de una palabra.

Ejemplo:

1.3.5. N| last_name, shipping_addresses | de datos como son tablas, store procedure, vista, columnas.

Ejemplo incorrecto:

Nomina23 /usp_ingresos238

Ejemplo correcto:

NOMINA /usp_ingresos

1.3.6. El nombre de los objetos de base de datos deberá estar escrito en singular y representar a la información que estará almacenando, para los esquemas el nombre deberá ser en mayúsculas y debe ser específico al igual deberá de tener una relación lógica con las tablas que agrupa.

Ejemplo para tablas de tipo catalogo:

tbl_cat_vehiculo

Ejemplo para esquemas:

FINANZAS

1.3.7. El nombre de los objetos de base de datos no deberá incluir caracteres especiales, por ejemplo: #, $, %, &, ?, !, +, *, {,], por citar algunas, incluyendo la letra "ñ", esta deberá de ser omitida.

1.3.8. Elegir palabras cortas y de máximo una o dos como sea posible.

1.3.9. Los nombres de los campos deberán ser comprensibles. Por ejemplo:

precio, nombre_compania

1.3.10. Evitar utilizar la columna con el mismo nombre que el nombre de la tabla. Esto puede causar confusión al escribir una consulta.

1.3.11. Evitar nombres abreviados, concatenados o basados en siglas.

1.3.12. Los nombres de tablas no deben tener rebasar el siguiente número de caracteres:

a) MySQL: 64 caracteres como máximo.
b) PostgreSQL: 63 caracteres como máximo.
c) Progress OE: 32 caracteres como máximo.
d) SQL Server: 128 caracteres como máximo.

1.3.13. Los nombres de las columnas deben estar en singular, incluyendo llaves foráneas.

1.3.14. Utilizar los siguientes prefijos dependiendo que tipo sea el dato de la columna:

a) VARCHAR(v) - Cadenas de texto finitas.
b) TEXT (txt)- Cadenas de texto no finitas.
c) INT(i) - Enteros en general.
d) BIGINT(bi) - Llaves primarias, foráneas y enteros muy grandes.
e) BIT(b) - Valores booleanos.
f) DATE(d) - Campos de fecha.
g) DATETIME(dt) - Campos de fecha y hora.

Ejemplo:

vnombre, dtfechaingreso, ifolio

1.3.15. Los nombres de los disparadores o "triggers" deben seguir el estándar ut_<nombre>.

Ejemplo:

ut_terminar

1.3.16. Los nombres de las vistas deben seguir el estándar vw_<nombre>. Ejemplo:

vw_vista

1.3.17. Los nombres de los procedimientos almacenados o "stored procedures" deben seguir el estándar usp_<nombre>, usar sp_ es un error. Ejemplo:

usp_empezar

1.3.18. Creación de tablas de Tipologías: Para el caso de Tablas que solamente contengan descripciones (por ejemplo, Tabla de Motivos) se deberá agregar un campo auto-numérico para identificar el registro. Normalmente las descripciones son también únicas. Para el actualizador de estas tablas no se deberá actualizar ni mostrar el campo identificador. Para la exportación a texto de esta tabla se deberá exportar el campo identificador para tener la referencia a las tablas que usen estos datos de descripción.

1.3.19. Para tablas relacionales que mantengan una gran cantidad de almacenamiento (superior a 2 TB de información), se debe establecer una estructura de particionamiento de forma obligatoria, por ejemplo, para el DBMS SQLSERVER sería la creación de FileGroup.

1.3.20. El uso de tablas NO relacionales debe hacerse bajo aprobación y supervisión de la Subsecretaria de Tecnologías de la información.

1.3.21. Los nombres de la tabla deberán iniciar con el tipo de información que maneja. Ejemplos:

cat_medicamento (catalogo) tbl_cliente_moroso (tablas)

1.3.22. Las tablas principales de las bases datos deben tener creados además de las llaves primarias, índices según la agrupación de búsqueda principal y acceso desde otras entidades o elementos de información.

1.3.23. Los índices se nombran considerando la tabla a la que están relacionados y el propósito del índice. Las claves primarias utilizan el texto "PK" como sufijo o prefijo, según se considere conveniente. Ejemplos:

```
PK_empleado
FK_trabajo
```

1.4. Gestión Documental

1.4.1. Para toda base de datos nueva que es entregada al departamento de base de datos, la persona responsable de la entrega (líder de cambio) deberá compartir el documento "Capacity Planning Database" en el cual deberá de contemplar las tablas más transaccionales, la estimación anual de crecimiento de cada tabla, los Store Procedure y vistas indispensables de la operación y su flujo de ejecución.

1.4.2. Para toda base de datos nueva que requiera una instalación y configuración en específico, será necesario que la persona solicitante (líder de cambio) proporcione al DBA el manual de instalación y configuración requerido.

1.4.3. Al finalizar la relación contractual con el empleado, es importante dar de baja a la cuenta de acceso a la base de datos que se le fue asignada, esta responsabilidad corresponde al jefe de área, ya que él es quien debe de notificar y solicitar por correo al área de base de datos la baja de la cuenta y revocación de permisos, enviando correo con el formato de solicitud de usuarios indicando la baja del usuario y con el folio del ticket correspondiente. Se tiene un lapso no mayor a siete días naturales para realizar este proceso.

1.4.4. El diseño de las tablas siempre debe estar acompañado de su modelo y diagrama actualizado desde el cual se pueda realizar seguimiento y visualización conceptual.

1.4.5. En todo script ya sea nuevo que haya sido actualizado, es indispensable anexar los comentarios al inicio de los Store Procedure, para que estos puedan guardarse dentro del cuerpo del Store Procedure y con ello llevar la bitácora de cambios. Ejemplo:

```
/*
Objetivo: <Descripción>
Creado por: <nombre del desarrollador/persona que crea el script >
Fecha creación: <fecha de creación >
Modificado por:
Última modificación: <Descripción>
Fecha modificación:
*/
```

1.4.6. Toda tabla nueva que sea creada o actualizada deberá de contar con su diccionario de datos, el cual debe de estar embebido en el código de creación y/o actualización.

1.4.7. Para toda solicitud de cambios, se deberá agregar el folio del ticket correspondiente dentro del formato de solicitud de cambios; y se deberá ser llenado con los datos del personal que aplicó el cambio.

1.4.8. Todo formato de solicitud de cambios deberá ser resguardado en una NAS o sitio accesible para todos los integrantes del equipo, así como los archivos requeridos para el cambio solicitado.

1.5. Scripts de base de datos

1.5.1. En el cuerpo del script se deberá de indicar el nombre de la base de datos en donde se estará ejecutando el script.

Ejemplo:

```
USE master
GO
SELECT TOP 1* FROM [dbo].[spt_monitor]
```

1.5.2. Todo script deberá incluir el manejador de errores.

1.5.3. Los scripts de base de datos deberán de ser guardados en formato .sql.

1.5.4. Evitar usar "SELECT * FROM", las consultas solo deberán de incluir las columnas necesarias, para agilizar la entrega de información al cliente. Con esto se evitará llevar información que no necesita el cliente, y prevenir que la red se sature.

1.5.5. Para consultas de listas de registros, usar el operador TOP n. Con esto se evita llevar muchos registros al cliente. También se descongestiona la red y para el cliente es más rápido.

1.5.6. Si se usa el operador UNION y se está seguro que ambas Querys NO tienen registros duplicados, entonces mejor usar UNION ALL, para evitar que implícitamente se haga uso del operador DISTINCT.

1.5.7. Evitar usar SELECT ... INTO table_name. Esto bloqueará tablas del sistema. En lugar de esto, crear primero las tablas y luego reescribir la sentencia como INSERT INTO table_name SELECT.

1.5.8. Si se va a leer data de una sola tabla, evitar hacerlo usando vistas que usan otras tablas.

1.5.9. Evitar el uso de sentencias SELECT con operaciones sobre los campos que va a obtener.

Ejemplo de este error:

```
Select convert (int(campo1)) + fn_funcion_propia(campo2, campo3)
```

1.5.10. Al escribir una consulta o "Query" usando una vista, evita leer una tabla referenciada en la vista. Ejemplo:

```
SELECT member_number, first_name, last_name, room_number FROM members WHERE state = 'A'
```

1.5.11. Al crear un script de inserción de datos, se deberá especificar las columnas a insertar información.

Ejemplo:

```
INSERT INTO tabla (campo1, campo2, ...) VALUES (...)
```

1.5.12. Escribir JOINS en formato ANSI (usar la cláusula JOIN ON). Con esto se asegura la escritura de todas las restricciones sin posibilidad de olvidar alguna.

1.5.13. Evitar usar la misma tabla más de una vez en un solo Query. Para mejorar esto, usar tablas temporales, se prefiere usar un JOIN en lugar de un sub-Query.

1.5.14. En lugar de usar una sentencia con muchos JOINS donde las tablas involucradas son grandes, crear una tabla temporal con los datos de la tabla principal (códigos) y luego actualizar esta tabla haciendo JOINS con las tablas secundarias.

1.5.15. En lugar de usar la cláusula IN conjuntamente con un sub-query, usar una sentencia JOIN.

Ejemplo:

```
SELECT pub_name FROM dbo.Publishers JOIN dbo.Titles ON Titles.pub_id = Publishers.pub_id
```

1.5.16. Evitar usar funciones sobre columnas en la cláusula WHERE.

Ejemplo de este error:

```
SELECT member_number, first_name, last_name FROM members WHERE dateofbirth
< DATEADD (yy,-21,GETDATE())
```

1.5.17. Si se usa LIKE en la cláusula WHERE, tratar de usar por lo menos 3 caracteres adelante.

Ejemplo:

```
SELECT customer_name FROM customers WHERE last_name LIKE 'abc%'
```

Ejemplo de este error:

```
SELECT customer_name FROM customers WHERE last_name LIKE '%abc'
```

1.5.19. Donde sea posible usa la cláusula BETWEEN en lugar de IN.

Ejemplo:

```
SELECT id_custome, customer_name FROM customer WHERE customer_number BETWEEN 1000 and 1004
```

1.5.20. Evitar el uso de hard-code (incrustar datos directamente en el código fuente del programa).

1.5.21. Evitar usar cursores. En su lugar, usar tablas temporales con un campo entero identity (1,1) o auto_increment el cual se podrá barrer en forma secuencial. No olvidar indexar el campo.

1.5.22. Otra forma de sustituir los cursores es mediante el uso de expresiones comunes de tabla (CTE).

1.5.23. Considerar que las funciones MIN y MAX pueden usar índices. Si es posible, crear índices sobre las columnas sobre las cuales se usan estas funciones. Cuando se usen tablas temporales, considerar crearles índices para aumentar el desempeño de sus Querys.

1.5.24. Cada Query deberá hacer uso de un índice sobre una columna que tenga una alta dispersión.

1.5.25. Si se va a actualizar, insertar o eliminar muchos registros en una sola sentencia, mejor hacerlo en partes pequeñas.

1.6. Transaccionalidad

1.6.1. Nunca romper una transacción en dos transacciones que sean invocadas consecutivamente desde el cliente. Esto hace que, si falla la segunda transacción, la base de datos quede corrupta.

1.6.2. Procurar que las transacciones sean pequeñas, es decir, que accedan a la menor cantidad de páginas de la base de datos.

1.6.3. Evitar declarar una sola gran transacción para los procesos en lote. Es mejor tener varias transacciones pequeñas y manejar reprocesos.

1.6.4. Evitar usar transacciones anidadas.

1.7. Respaldos de base de datos

1.7.1. Todas las bases de datos deberán contar con la programación de tareas de respaldos de base de datos, al menos deberán contar con un respaldo full diario.

1.7.2. Todos los días el personal encargado de la creación de los respaldos de base de datos, deberá de revisar que las tareas se hayan ejecutado sin errores y que los respaldos se encuentren

alojados tanto dentro del servidor de base de datos como en la unidad o servidor dedicado especialmente para los respaldos de base de datos.

1.7.3. Los respaldos de base de datos, deberán ser validados a diario por el área responsable de ello, para garantizar que estos estén íntegros y que, en caso de algún incidente o desastre natural, estos puedan ser restaurados sin contratiempos.

1.7.4. En caso de que se presente un problema con el Hardware, se deberá de notificar al área correspondiente encargado de administrar los servidores, para su revisión y seguimiento.

1.7.5. Si el problema presentado es con la base de datos, el área de Administración de Base de Datos, deberá de validar y solucionar el incidente en el período acordado.

1.8. Mantenimientos de Bases de Datos

Para mantener un sistema de base de datos en buen estado y garantizar un rendimiento coherente es necesario llevar a cabo un mantenimiento al menos una vez al mes a todas las bases de datos, exceptuando las bases Progress deben realizare al menos una vez al año.

Las tareas que se deben considerar aplicar de acuerdo al DBMS son:

- Las tareas de mantenimiento a realizar en base de datos con DBMS Progress son:
  - Re-indexado de los índices de base de datos (idxrebuild)
  - Truncado del Before Image (BI)
  - Truncado del Log de base de datos
  - Análisis de base de datos (idxanalys)
  - Análisis de índices de base de datos (idxcheck)
  - Mover tablas de base de datos (tablemove)
  - Movimiento de índice de un área a otra (idxmove)
  - Compactar índices de base de datos (idxcompact)
- Las tareas de mantenimiento a realizar en base de datos con DBMS SQL son:
  - Actualización de estadísticas
  - Purgado de Log
  - Reindexado
  - Reducción del tamaño de archivos

Para otros DBMS se podrán realizar tareas de mantenimiento derivadas de observaciones durante el monitoreo del estado de la base o bajo solicitud al Administrador de la base de datos.

1.9. Monitoreo de las Bases de Datos

Se deberá de realizar el monitoreo diario a las bases de datos después de haber ejecutado el mantenimiento por un periodo de una semana, en el monitoreo se deberá de revisar los siguientes puntos:

1.9.1. Comportamiento de la base de datos:

- Validar con el área funcional la velocidad de respuesta de la base de datos, comparado con el tiempo de respuesta antes del mantenimiento.

1.9.2. Crecimiento de las áreas de datos.

- Este punto se deberá de monitorear a diario y registrar el crecimiento en una bitácora de base de datos.

1.9.3. Estadística de base de datos.

- Se deberá ejecutar el análisis de la estadística de base de datos después de haber implementado el mantenimiento a la base de datos, para obtener el tamaño recuperado en disco.

1.10. Nivel de Criticidad de los Servicios Especializado de Bases de Datos

El Administrador de Base de Datos debe valorar las acciones a realizar en una base de datos considerando el nivel de impacto que representa su aplicación. Estos niveles pueden definirse de la siguiente manera:

- Nivel de criticidad ALTO: Se considera un nivel de criticidad Alto cuando las operaciones están detenidas, cuando las cajas no pueden iniciar su sistema o ninguna entidad o secretaría puede ingresar al sistema SIGEY. Por lo cual el no aplicarlo tendría repercusiones graves. Su ejecución es inmediata.
- Nivel de criticidad MEDIA: Se considera un nivel de criticidad Media cuando se requiere implementar una mejora, un nuevo módulo en el sistema, nuevos objetos para un proyecto nuevo. Su ejecución se estaría realizando en el horario nocturno establecido por el área de base de datos.
- Nivel de criticidad BAJA: Se considera un nivel crítico Bajo cuando se requiere implementar nuevos módulos, mejoras en la base de datos o sistemas para verse reflejados en días posteriores, por lo cual se pueden ejecutar en fines de semana en horario nocturno.

RENACIMIENTO MAYA YUCATÁN GOBIERNO DEL ESTADO : 2024 - 2030	**SECRETARÍA DE ADMINISTRACIÓN Y FINANZAS** Dirección de Desarrollo de Plataformas	
Solicitud de Alta de Servicio en la Capa de Seguridad		

Persona que solicita			
Nombre y Apellido:			
Departamento:		**Puesto:**	
Jefe inmediato:			
Fecha solicitud:	04/04/2025	**Correo:**	
Teléfono:		**Extensión:**	
Información del Servicio Web			
Clave del WS:		**Nombre del WS:**	
URL base:		**NameSpace:**	

Métodos del Servicio Web			
Metodo #1			
Nombre:		**Nombre interno:**	
Método:	Elija un elemento.	**Respuesta:**	Elija un elemento.
☒ **Enviar token**		**Variable del token:**	
Metodo #2			
Nombre:		**Nombre interno:**	
Método:	Elija un elemento.	**Respuesta:**	Elija un elemento.
☒ **Enviar token**		**Variable del token:**	
Metodo #3			
Nombre:		**Nombre interno:**	
Método:	Elija un elemento.	**Respuesta:**	Elija un elemento.
☒ **Enviar token**		**Variable del token:**	

Nombre y firma del Solicitante

MEDIDAS DE SEGURIDAD PARA PLATAFORMAS DIGITALES

ÍNDICE

		Página
I.	**OBJETIVO**	**2**
II.	**ALCANCE**	**2**
III.	**CONTENIDO DE LA GUÍA**	**3**

I. Objetivo

Promover la aplicación de medidas de seguridad para procurar la protección de las plataformas digitales del Gobierno del Estado de Yucatán, así como generar confianza a la ciudadanía en su interacción con el Gobierno.

II. Alcance

Aplica a la Subsecretaría de Tecnologías de la Información y Comunicaciones de la Secretaría de Administración y Finanzas, así como a las Dependencias y Entidades y desarrolladores externos que fueran a realizar el desarrollo de plataformas digitales del Gobierno del Estado.

III. Contenido de la Guía

Las plataformas digitales como los son páginas web, sistemas o aplicaciones móviles, interactúan con los usuarios y gestionan información de relevancia relacionada con la operación del gobierno del estado por tanto en esta guía se presentan las consideraciones que deben contemplarse para reducir la probabilidad de que se vean vulnerados durante su interacción.

Dichas consideraciones son:

1. Control de acceso a usuarios
2. Registros de actividades y su resguardo
3. Validación básica de paso de parámetros y formularios
4. Content Security Police (CSP)
5. Ocultamiento de mensajes de error y debug
6. Subida de archivos
7. Aislamiento de servidores de producción. DMZ
8. Uso de cifrado SSL
9. Respaldos
10. Security checkups

1. Control de acceso a usuarios

1.1 Passwords

Las contraseñas de acceso pueden encontrarse en diferentes instancias en el proceso de hospedaje de un sitio web, transversalmente, los diferentes dueños de procesos deben tener en cuenta las siguientes consideraciones, ya sea en las contraseñas de acceso a la plataforma, al sistema operativo, el usuario con el que corre el servicio, el usuario para la conexión de la base dedatos o de la API, etc., deben ser contraseñas fuertes, en el entendido de que una contraseña fuerte debe contar con los siguientes componentes:

- Longitud mínima requerida. - Lo habitual es al menos 10 caracteres para evitar descubrimiento rápido por permutación de caracteres, idealmente 12 o más caracteres.
- Mayúsculas. – Duplica el set de caracteres a evaluar, si se utiliza en combinación con minúsculas.
- Minúsculas. – Duplica el set de caracteres a evaluar, si se utiliza en combinación con mayúsculas.
- Caracteres Especiales, incluyendo espacios en blanco. – La intención es incrementar la

aleatoriedad de la posición de un elemento adicional y un juegode caracteres ampliado.

- Números. - Incrementa el set de caracteres a evaluar, si se utiliza en combinación con mayúsculas o minúsculas.
- Complejidad. – Probablemente la más difícil de considerar, ya que por costumbre utilizamos técnicas para recordar las contraseñas, la aleatoriedadpuede incrementar el tiempo de convergencia de algoritmos de fuerza bruta, sin embargo, si es suficientemente corta no tiene mucha ventaja contraalgoritmos secuenciales de fuerza bruta.

Frase desafío. (Passphrase).

La frase desafío se utiliza comúnmente como una contraseña fuerte, consiste en aprovechar la habilidad nemónica del ser humano para poder referenciar una frase semi encriptada, como ejemplopodemos decir que una contraseña fuerte de acuerdo a los componentes descritos puede ser:

Contraseña	Complejidad	Romper Encriptación
"Gobierno0"	Buena	42 minutos
"Gobierno.0"	Fuerte	10 años
"G0b13rn0.0"	Muy fuerte	10 años
"Gobierno cero.0"	Muy fuerte	34 billones de años
"G0b13rn0 Un0. C3ro"	Muy fuerte	64 billones de años

En el ejemplo, el tiempo que llevaría romper la encriptación hipotéticamente sería utilizando un algoritmo mono proceso serial, las técnicas actuales pueden hacer que equipos poderosos en recursos disminuyan este tiempo estimado. No obstante, queda claro en la comparación, el beneficio de la complejidad de una frase desafío contra una contraseña tradicional, aunado a la facilidad de recordar la frase Contraseñas de diccionario.

Existen aplicaciones que se dedican a probar sistemas de autenticación enviando por script las instrucciones de un intento de acceso, y apoyados en bases de datos de contraseñas comunes, conocidas y combinaciones de las mismas. Programas malintencionados (malware) contribuyen a la alimentación y enriquecimiento de estas bases de datos tomando datos del usuario como el nombreo fechas que existan en documentos y agregándolas al diccionario, algunas muestras de diccionarioson accesibles desde internet, una buena práctica consiste en no utilizar contraseñas que incluyanpalabras que existan en alguna muestra de diccionario, o que asemejen un patrón establecido porestas palabras diccionario. Algunos de los ejemplos más comunes de contraseñas diccionario (idioma inglés):

123456	111111	princess	football	Charlie

password	1234567	admin	123123	aa123456
123456789	sunshine	welcome	monkey	Donald
12345678	Qwerty	666666	654321	password1
12345	Iloveyou	abc123	!@#$%^&*	qwerty123

1.2 Compartición de contraseñas

Las contraseñas no deber compartirse entre áreas, usuarios, servicios o aplicaciones, deben ser únicas cada en cualquier etapa del flujo de la construcción y funcionamiento de una plataformaweb. Si el servicio que protegen es de acceso privilegiado, deben ser aún más robustas conforme a lo revisado en el punto anterior, por lo que se requiere que cualquier persona involucrada en el desarrollo, administración, mantenimiento o actualización deben contar con algún gestor de contraseñas que cuente con medidas mínimas de seguridad como la encriptación, protegido por una contraseña maestra, donde se almacenarán las diferentes contraseñas que puedan requerirse en el cumplimiento de sus funciones. Las contraseñas de sistema o globales (cuentas privilegiadas) deben estar documentadas y debidamente resguardadas pues comprometen la continuidad del servicio de la plataforma web.Software actualizado.

Se reconoce que el intercambio de contraseñas puede ser necesario en circunstancias **excepcionales** durante el desarrollo de aplicaciones, como en casos de soporte técnico urgente, resolución de errores críticos o acceso temporal a sistemas compartidos. Sin embargo, debido a los riesgos de seguridad asociados, esta práctica debe ser estrictamente regulada y limitada.

a. Restricción General:

El intercambio de contraseñas está prohibido salvo en situaciones excepcionales aprobadas por escrito por el responsable del equipo o el administrador de sistemas. Se debe priorizar el uso de herramientas de gestión de acceso (como sistemas de autenticación multifactor, claves temporales o permisos delegados) antes de recurrir al intercambio directo de credenciales.

b. Criterios para la Excepción:

- El acceso debe ser esencial para resolver un problema crítico que afecte el desarrollo o funcionamiento de la aplicación.
- No debe existir una alternativa viable para otorgar acceso sin compartir la contraseña.
- La solicitud debe ser aprobada previamente por el supervisor del proyecto o el

responsable de seguridad.

c. Procedimiento para Compartir Contraseñas:

- Solicitud Formal: El solicitante debe presentar una justificación por escrito (correo electrónico o formulario interno) detallando el motivo, el sistema involucrado y la duración estimada del acceso.
- Canal Seguro: La contraseña solo podrá compartirse a través de un medio cifrado y efímero (como un gestor de contraseñas autorizado con acceso temporal o un mensaje cifrado que se autodestruya). Nunca se debe enviar por correo electrónico no cifrado, mensajería instantánea o cualquier otro medio no seguro.
- Cambio Inmediato: Una vez finalizado el uso, la contraseña compartida debe cambiarse de inmediato por una nueva, siguiendo las políticas de seguridad (mínimo de caracteres, complejidad, etc.).

d. Registro y Auditoría:

- Todo intercambio de contraseñas debe documentarse, incluyendo: nombre del solicitante, motivo, fecha, hora y sistema afectado.
- El responsable de seguridad revisará periódicamente estos registros para garantizar el cumplimiento de la política.

e. Responsabilidades:

- El propietario de la contraseña es responsable de notificar al equipo de seguridad tras el intercambio y de coordinar el cambio de la misma.
- El receptor de la contraseña debe utilizarla únicamente para el propósito aprobado y no almacenarla ni divulgarla a terceros.

f. Consecuencias del Incumplimiento:

Cualquier violación de esta política, como compartir contraseñas sin autorización o no seguir el procedimiento establecido, será considerada una falta grave y podrá derivar en acciones disciplinarias, de acuerdo con las normativas internas de la función pública.

Las plataformas de sistema operativo, servidor web, interprete CGI, APIs de desarrollo, paquetes decompilación, librerías de uso público, frameworks de diseño y de scripting, etc, son elementos que comúnmente se encuentran en la composición de una plataforma web.

Las actualizaciones de cada uno de éstos componentes, no solamente incluyen mejoras o adicionesa las características funcionales, sino que también consideran las correcciones

de algunos bugs deseguridad, los cuales casi siempre se encuentran documentados. Un atacante puede utilizar la información disponible para una vulnerabilidad específica existente en una versión desactualizada para ganar acceso y privilegios a través de la falla. Contar con un esquema de actualización de paquetes y parches es necesario para conservar una pequeña ventaja en la posibilidad de tener vulnerabilidades bien conocidas y bien documentadas.

2. **Registros de actividades y su resguardo**

Los archivos de registro de actividades pueden ser de lo más variado, desde el sistema operativo, intérprete, e incluso en el desarrollo del mismo código de la plataforma pueden existir elementos que constantemente registran en archivos de texto las actividades de cada componente. Éstos elementos de registro son conocidos comúnmente con el nombre de ***Logs***. Se debe contar con unprocedimiento que garantice la integridad de estos registros, incluso el respaldo remoto de los mismos. Esto permite trazabilidad y evidencia en caso de algún incidente.

3. **Validación básica de paso de parámetros y formularios**

3.1 Paso de parámetros

Si es requerido el paso de parámetros, se prefiere el paso de parámetros sensibles mediante el método POST, respetando los requerimientos y mejores prácticas del área de desarrollo involucrado, pues presenta ligeramente mejores beneficios en el tema de seguridad ya que uno pasalos parámetros y sus valores en la URL (GET) y el otro lo hace dentro del cuerpo del código (POST),como referencia, presentamos a continuación algunas diferencias clave entre los métodos GET yPOST.

Acción	GET	POST
Botón Retroceder / Recargar	Sin Efecto	Los datos serán reenviados (el navegador deberá advertir al usuario de esta situación)
Añadir a Favoritos	Se permite, la URL y parámetros quedarán como un acceso directo.	No se pueden agregar los parámetros a una URL de favoritos.
Cache	Los datos se almacenan en cache.	No se almacena en cache.
Encoding type	application/x-www-form-urlencoded	application/x-www-form-urlencoded o multipart/form-data. (Utiliza multipart encoding para datos binarios)

Historial	Los parámetros quedan almacenados en el historial del navegador.	Los parámetros no son almacenados en el historial del navegador.
Restricciones en longitud de datos.	Si, cuando se envían datos, el método GET agrega los datos a la URL; y la longitud de la URL es limitada (2048 caracteres, y muchos menos caracteres bajo esquemas de protección de equipos firewall).	No hay restricciones.
Restricciones entipos de datos	Solamente caracteres ASCII son admitidos	No hay restricciones, se admiten datos binarios.
Seguridad	El método GET es menos seguro, comparado con el método POST porque los datos enviados son parte de la URL.	El método POST es un poco más seguro que el método GET, debido a que los parámetros no son almacenados en el navegador, historial, ni en los logs del servidor.
Visibilidad.	Los datos de los parámetros son visibles para todos, por estar en la URL.	Los datos no son visibles en la URL

3.2 Validación de controles input

Adicionalmente, los parámetros pueden estar accionados por el código de la plataforma, como procedimiento interno, un aspecto importante es que los valores de algunos parámetros requierenla entrada del usuario, esta entrada de datos se realiza por controles input de formularios web.

Los controles input de formularios web, son susceptibles a ser descuidados en las etapas finales devalidación al liberar un sitio, un input sin la validación de las cadenas que se almacenan en el valor, puede pasar parámetros directamente al siguiente motor de evaluación, dentro de los cuales, losmás comunes son los siguientes:

- SQL Injection.
- XSS attacks.

La mejor manera de mitigar estos riesgos es contar con un procedimiento para validar, escapar y moldear los valores recibidos en un input, antes de pasarlos como parámetros a la siguiente etapade ejecución. Aplica también a la impresión de valores almacenados en la BD, ya que, en caso de almacenarse una instrucción maliciosa en la BD, la impresión del valor, como un código script, porejemplo, pasaría al motor de ejecución sin ser ésta la intención del funcionamiento de la plataformadesarrollada.

- **SQL Injection**

Consiste en el paso malintencionado de comandos SQL al motor intérprete encargado de ejecutar dichos comandos sobre la base de datos, de esta manera, se pretende explotar la lógica de programación creada para la consulta o almacenamiento de un valor, o almacenar instrucciones en la BD, para que sean ejecutadas al imprimir el valor en otra consulta.

Se pretende entonces, prevenir el agregar al dato en el input, un valor que siempre resulte verdadero, permitiendo a la consulta ejecutar la consulta independientemente de que el valor seaválido o existente, una variante consiste en añadir una instrucción SQL al valor, pretendiendo que se ejecute como si fuera parte de la consulta original, a modo de procesamiento por lotes de las instrucciones.

Consulta en código CGI	Valor esperado	Valor malintencionado	Resultado esperado	Resultado malintencionado
SELECT * FROM Users WHERE UserId =	105	105 OR 1=1	Dataset: John Smit.	Dataset: All Table Users
SELECT * FROM Users WHERE Name ="John Doe" AND Pass = "myPass"	John, Doe	" or ""=", "or ""="	Dataset: John Doe	Dataset: All Table Users
SELECT * FROM Users WHERE UserId =	105	105; DROP TABLE Suppliers	Dataset: John Smit.	Dataset: John Smit, Eliminacion de tabla Suppliers

Una buena práctica consiste en la parametrización del valor en la consulta interna codificada, evitando ejecuciones de SQL no intencionales. Otra buena práctica consiste en la limpieza de lascadenas pasadas como parámetros, eliminando caracteres de las cadenas de texto en el valor, que sean interpretados por el lenguaje SQL, como operadores. Un ejemplo son los símbolos de operadores (%=;|"><$&+-/.?) AND, OR, LIKE.

- **Ataques XSS**

Como en el caso anterior, el ataque consiste en explotar la falta de validación de cadenas en los controles input de los formularios, para intentar pasar instrucciones de script activo, sean jquery,javascript, vbscript, e incluso instrucciones CGI (por ejemplo <?php echo ""?>), en la expectativa de que el siguiente motor interprete las instrucciones como parte del código original.

Un ejemplo de esto sería pasar una instrucción meta redirect de un control input, al almacenamiento en la BD de la plataforma, esta instrucción puede ser impresa en un listado, cuando el jquery intentedarle formato a la lista, ejecutará también la instrucción impresa. Este comportamiento pudiera ser aprovechado para suplantar la plataforma legitima por una versión falsificada de la misma, intentando obtener valores que un usuario inadvertidamente introduzca, pensando que se encuentra en la plataforma original. Una prueba simple es introducir instrucciones echo o print en los controles de input para observar si poseen esta vulnerabilidad.

Para ambos casos, SQL injection y XSS Attack, siempre es recomendable que las validaciones a las cadenas de los controles input sean realizadas tanto del lado cliente como en el servidor que recibeel parámetro.

4. **Content Security Police (CSP)**

Las cabeceras de respuesta Content-Security-Policy, se presentan en la repuesta del servidor de laplataforma web, un cliente compatible reforzará la declaración de la política de lista blanca del navegador. Por ejemplo, se puede incluir en la política una ejecución de código JavaScipt más estricta, tratando de prevenir ataques XSS, en realidad esta implementación conlleva una serie decaracterísticas que son desactivadas por default:

- Código JavaScript inline.
  - Bloques <script>
  - Manejadores de evento DOM como atributos html (como por ejemplo .onclick)
  - Ligas URL javascript: (en la barra URL)
- Indicaciones de CSS inline.
  - Bloques <style>
  - Atributos style en elementos html
- Evaluación de código dinámico.
  - eval()
  - argumentos de texto para las funciones setTimeout y setInterval
  - el constructor new Function()
- Instrucciones CSS dinámicas.
  - El método CSSStylesheet.insertRule()

Desarrollar una plataforma nueva mientras se utiliza una CSP es un desafío, pero existen plataformas de desarrollo compatibles con CSP, es un hecho que muchas aplicaciones existentes deben cumplir rediseño o una política CSP no tan severa. La recomendación de buena práctica esutilizar el código CSS y script mediante las llamadas de carga de archivos externos (<script src>), interpretar vía JSON en vez de evaluarlos y utilizar EventTarget.addEventListener() para asignar manejadores de eventos.

5. **Ocultamiento de mensajes de error y debug**

El ocultamiento de mensajes de error y de depuración, en una buena práctica por si misma, ya que ayuda a minimizar la información acerca de la plataforma en la que se ejecuta o se encuentra desarrollada la plataforma. De este modo dificulta al operador malintencionado, hacerse de información acerca de la versión, plataforma, web server o CGI sobre los cuales se ejecuta la aplicación.

Debe existir dentro del procedimiento de liberación de una plataforma web, una etapa que sea dedicada a la validación del ocultamiento de los mensajes de error tipo y mensajes de depuración. Si debe existir mensajes de error, deben ser los mensajes desarrollados para este fin específico, con mensajes propios del desarrollo y no del sistema.

6. **Subida de archivos**

Se recomienda no utilizar métodos que permitan subir archivos al servidor mediante la plataforma web. Si no existe una alternativa, existen algunas consideraciones que se vuelven obligatorias en su implementación:

- Remoción de privilegios de ejecución del archivo.
- Renombramiento de las extensiones del archivo vía validación.
- Validación de existencia de comandos de ejecución en archivos de texto plano.

En la medida que algunos controles no puedan ser del todo implementado, se requiere considerarlas implicaciones que conlleva la escritura de un archivo tipo script o shell en las carpetas del servidor, y de cómo esto representa una posibilidad latente de secuestro del servidor o permita otorgar puertas traseras al servidor mediante ejecución de comandos al nivel del sistema operativo.

7. **Aislamiento de servidores de producción (DMZ)**

La infraestructura de procesamiento debe ejecutarse en un entorno que esté monitoreado, que sus accesos puedan ser regulados y que se puedan determinar y clasificar intentos de conexiones no relacionadas al servicio que proporciona. Este entorno muchas veces se denomina DMZ (*demilitarized zone).* El concepto sugiere que los servidores puedan tener acceso a internet para la publicación de sus servicios, al mismo tiempo que el acceso de los mismos servidores hacia la red interna se encuentra restringido, de modo tal que, en caso de comprometer un servidor alojado en la DMZ, no se compromete el acceso hacia los recursos de la red interna.

8. **Uso de cifrado SSL**

El sitio debe seguir las recomendaciones para ser hospedado mediante el servicio de https, cada vez más motores de búsqueda e indexación favorecen los resultados a los sitios que si cuentan con https sobre los que no lo hacen. Adicionalmente el servicio se ofrece cifrado de punto a puntoentre el navegador visitante y la plataforma, dificultando la captura de datos al escuchar el medio detransporte.

9. **Respaldos**

Se debe contar con un esquema que permita la recuperación en caso de incidentes sobre los componentes que soportan la plataforma web, en esencia, se debe contar con un esquema de respaldos que garanticen la integridad del código fuente, parámetros operativos del servidor, BD y webservice. Así como el control de las versiones de los elementos de librería utilizados. Se debe considerar respaldar, para recuperación en caso de falla:

- El código fuente de la plataforma.
- El código de las librerías y plataformas.
- Los instaladores del software de desarrollo.
- Bases de datos.
- Parámetros operativos de:
  - Sistema operativo
  - Web Server
  - Syslog
  - Sistema de administración de BD.

10. **Security checkups**

Se debe considerar la tarea de realizar security checkups sobre las plataformas desarrolladas, estaspruebas pueden realizarse en coordinación con el equipo de seguridad informática, los resultadospueden arrojar posibles puntos de mejora, en caso de no ser aceptable el riesgo evaluado tras el uso de estos checkups.

Algunas plataformas que pueden utilizarse para la realización de los security checkups:

- Netsparker
- OpenVAS
- Security Headers – IO
- Xenotix XSS Exploit Framework.

(resultado de https://securityheaders.com/?q=www.yucatan.gob.mx&followRedirects=on)