01 Estándar técnico de controles mínimos de seguridad de la información

Estándar técnico de controles mínimos de seguridad de la información

Este estándar tiene por objetivo definir una línea base de medidas para la protección de los activos de información, la información y los datos, tendientes a preservar su confidencialidad, integridad y disponibilidad, considerando las amenazas, peligros, usos indebidos y posibles ilícitos a los que están expuestos derivado de su adquisición, arrendamiento, desarrollo e implementación en las Dependencias y Entidades, y contribuir a una prestación de los servicios institucionales de una manera efectiva, ininterrumpida, organizada y responsable.

Los controles mínimos de seguridad de la información que se deben observar se indican para las etapas de planeación y gestión del proceso de implementación de la seguridad de la información, así como para diversos rubros tecnológicos.

Planeación

Desarrollar un procedimiento de gestión y tratamiento de riesgos de seguridad y, de acuerdo a su resultado, implementar las acciones preventivas y correctivas correspondientes.

Crear, probar e implementar el plan de respuesta y gestión de los incidentes de seguridad, que incluya la conformación del ERISC, así como las acciones de preparación, detección y análisis, contención, erradicación y recuperación, y actividades posteriores al incidente.

Crear, probar e implementar los planes de continuidad de operaciones y recuperación ante desastres, incluyendo en éste una lista predefinida y prioridades para su recuperación; cuando sea

posible, contar con sitios alternos como alternativa de recuperación.

Crear, probar e implementar el plan de gestión de las vulnerabilidades encontradas, en éste se deberá establecer el proceso para su identificación, asignación de responsables y tiempos para su solución.

Crear e implementar una matriz de relación de proveedores de servicios, estableciendo un inventario de proveedores y servicios, los acuerdos de niveles de servicio y las personas responsables.

Crear, probar e implementar el plan de migración de las aplicaciones obsoletas y/o de software con el ciclo de vida concluido.

Crear e implementar un plan de migración a software libre y estándares abiertos.

Gestión
Definir procesos y procedimientos que establezcan los pasos y tiempos para el respaldo de información y para las pruebas de restauración que le permita a la Dependencia o Entidad mantener su confidencialidad, integridad y disponibilidad. Implementar un programa de concienciación, formación y educación continua sobre seguridad de la información y el uso aceptable de los activos para todo el personal en la Dependencia o Entidad, como mínimo, se deberán considerar lo siguiente: Tópicos acerca de cómo interactuar de manera segura con los activos de información en general y los datos de la Dependencia o Entidad, identificar y almacenar, transferir, archivar datos confidenciales de manera adecuada y aplicar los procedimientos para el respaldo de información y copias de seguridad; Concienciación de las causas de la exposición voluntaria e involuntaria de datos para que se tenga la habilidad de reconocer los ataques más comunes, como son: la ingeniería social y el phishing, por mencionar algunos; asimismo, la composición de

contraseñas, administración de credenciales y autenticación multifactor (MFA).

Advertir sobre los peligros del descuido de los puestos de trabajo, conectarse y transmitir datos a través de redes inseguras para actividades de la Dependencia o Entidad y para reconocer un posible evento o incidente de seguridad, pérdida y robo de los activos de información y el reporte correspondiente.

Establecer políticas de contraseñas para la administración de TICs. Con un mínimo de 17 caracteres y renovación periódica, al menos cada 3 meses.

Implementar y utilizar autenticación multifactor en los equipos, sistemas y aplicaciones donde sea necesario y posible.

Establecer el ciclo de vida de las credenciales de acceso, definiendo los procedimientos para su creación, uso, suspensión por inactividad y borrado en los sistemas y aplicaciones institucionales y cualquier otro activo de información donde se encuentran habilitadas.

Evitar el uso desmedido de cuentas de administración y cuentas privilegiadas, que puedan provocar algún daño a los activos de información o interrupción de los servicios institucionales con alto impacto a la operación y la continuidad. Utilizar protocolos de autenticación de rede*s.*

Deshabilitar las cuentas predeterminadas o genéricas en los activos de información para evitar el uso indebido. En caso de ser necesarias para la ejecución de ciertas tareas, aplicaciones o servicios, se deberá establecer el procedimiento para justificar, documentar, aprobar su uso y para contar con trazabilidad acerca de su uso por personas servidoras públicas y otras externas a las Dependencias y Entidades.

Administrar los accesos físicos a los activos de información, para garantizar su protección y la trazabilidad en los ingresos, por medio de señalamientos para la restricción del acceso físico a personas no autorizadas, internas y externas, y aplicando el uso de bitácoras de control para el acceso a instalaciones o áreas específicas.

Administrar los accesos lógicos a los activos de información, definiendo e implementando las reglas de control de acceso necesarias basadas al menos en usuarios y contraseñas, y con los privilegios necesarios de acuerdo a su perfil o rol Institucional, cuando sea posible, establecer los controles para el uso de la firma electrónica o la autenticación multifactor, gestionando los accesos por VPN e implementando las restricciones de acceso a nivel de puerto o de dirección física. Aplicar la adecuada configuración para la navegación web a fin de prevenir el acceso o, en su caso, detectar páginas fraudulentas o sospechosas en función de su reputación. Configurar adecuadamente el envío y recepción de correos electrónicos evitando la entrada y salida hacia dominios públicos o privados diferentes a los autorizados, se recomienda que preferentemente sea sólo entre el dominio Institucional y con otras entidades gubernamentales con las cuales se tenga comunicación interinstitucional. Para correo electrónico, implementar medidas antispam con la finalidad de evitar la propagación de malware, robo de datos y otras amenazas. Realizar el monitoreo constante que permita detectar conexiones, redes, dispositivos y software no autorizados realizado por personas internas o externas a la Dependencia o Entidad. Contar con un inventario actualizado de bienes y servicios de TIC, incluyendo en éste los equipos de cómputo, dispositivos de red, sistemas, aplicaciones y todos los que se definan.
Recursos Humanos
El personal que tenga acceso a información confidencial de la Dependencia o Entidad deberá firmar un acuerdo de confidencialidad y no divulgación de la información institucional. Establecer procedimientos para otorgar permisos y privilegios de acceso a los activos de información específicos, estableciendo roles y responsabilidades definidas para todas las personas servidoras públicas y proveedores usuarios de estos.

Reforzar el buen uso de la cuenta de correo Institucional para que todas las comunicaciones estén relacionadas con su encargo o función, informando de los riesgos y sanciones por incumplimiento.

Garantizar la asignación, revocación, supresión o modificación de los privilegios de acceso a los activos en materia de TIC, otorgados a servidores públicos de la Institución y de otras Dependencias y Entidades, así como al personal de los proveedores de servicios u otros usuarios, al inicio o término de su empleo, cargo o comisión, relación contractual o de cualquier otra naturaleza, o bien, cuando por algún motivo, el nivel de privilegios de acceso asignado cambie.

Elaborar un proceso y procedimiento de desvinculación del personal que considere, como mínimo: la devolución de los activos de información bajo custodia, el retiro de credenciales y las cuentas de acceso a servicios y sistemas que permitan poner en riesgo la seguridad de la información en la Dependencia o Entidad.

Contar con un proceso disciplinario, formalmente establecido y aceptado por todas las áreas de la Dependencias o Entidad, en el que se contemplen las sanciones administrativas o legales para los casos en los que el personal, interno o externo, incumpla con lo definido en materia de seguridad de la información.

Equipos físicos

Mantener un registro de todos los equipos físicos, la persona servidora pública responsable del mismo y sus fechas de garantía o finalización del servicio.

Mantener el firmware de los equipos actualizado, con la última versión estable indicada por el fabricante, sin comprometer la operación.

Mantener una bitácora de control de mantenimiento físico, cambio, remoción, o en su caso, la destrucción de los equipos y/o activos de información, estableciendo las fechas próximas en las que se deberá realizar.

Centros de Datos

Establecer una bitácora de control de acceso físico al centro de datos y a los activos de información esenciales, describiendo la actividad a realizar en estos.

Restringir el acceso físico a personas internas o externas, y permitirlo únicamente con autorización escrita y los registros correspondientes.

Implementar bóvedas de medios, centros de datos alternos cuando sea posible, servicios en la nube, como alternativas para recuperar la operación de los Centros de Datos ante alguna situación que los afecte o interrumpa.

En caso de requerirse la implementación de centros de datos alternos y bóvedas de medios, estos deberán estar localizados en distintos puntos geográficos, geológicamente viables y dentro del territorio nacional.

Implementar mecanismos de cifrado en los medios de almacenamiento en Centros de Datos centralizados, determinando que la administración de dichos mecanismos de cifrado esté a cargo de servidores públicos.

Todo Centro de Datos deberá cumplir en su diseño, estructura, desempeño, fiabilidad y medidas de seguridad equivalentes, como mínimo, el equivalente a una certificación TIER II.

Establecer los procesos o procedimientos formales para la administración del Centro de Datos, en cuanto a accesos, mantenimiento de equipos, supervisión de trabajos externos y otras actividades relacionadas.

Redes y Telecomunicaciones

Aplicar políticas de firewall permitiendo sólo el tráfico válido para la Dependencia o Entidad por medio de los puertos TCP/IP necesarios y autorizados.

Utilizar redes abiertas únicamente al proporcionar servicios a la población, las cuales deberán estar separadas y aisladas de las redes de datos institucionales, por ejemplo LAN, DMZ, invitados y de control, en caso de existir.

Utilizar mecanismos de cifrado de llave pública y privada, canales cifrados de comunicación y, cuando corresponda, de firma electrónica avanzada, que permitan el acceso de la información únicamente al destinatario autorizado al que esté dirigida.

Implementar controles de red como segmentación de redes, reglas de control de acceso, almacenamiento de bitácoras, seguridad de puertos, así como otras buenas prácticas con la finalidad de tener una mejor administración y seguridad en la red.

Desactivar el uso del protocolo RDP en general, en caso de ser necesario, limitarlo por velocidad con doble factor de autenticación, se recomienda hacer uso de redes privadas virtuales VPN.

Establecer accesos por VPN como único medio de acceso remoto a las redes internas de la Dependencia o Entidad, con autenticación separada a la de los servicios institucionales, sin tener permisos superiores a los que el usuario tiene en la red interna, y con la finalidad de que sólo usuarios autorizados puedan acceder a la red institucional desde sitios remotos.

Establecer acceso restringido a la red LAN para que sólo personal de la Dependencias o Entidad tenga acceso; para usuarios externos, será requerido contar con justificación, autorización y los registros correspondientes.

Implementar proxy en las redes wireless y LAN, estableciendo políticas de uso de la red, es decir, autorización para navegar a sitios de la Internet y no permitiendo el acceso o salida directa hacia ésta; además, se deberán detectar páginas fraudulentas o sospechosas por medio de direcciones IP o dominios.

Mantener una bitácora con la justificación de cada regla configurada en los firewall.

Deshabilitar las reglas de acceso en el Firewall que no sean ocupadas, verificarlas y actualizarlas periódicamente según las necesidades institucionales.

Establecer una configuración base y realizar periódicamente copias de seguridad de las configuraciones de dispositivos de telecomunicaciones.

Se deberá mantener regularmente actualizado el firmware, el sistema operativo y el software instalado en los equipos, en su última versión estable,sin afectar la operación, así como aplicar los parches de seguridad recomendados por los fabricantes.

Monitorear y analizar el flujo de tráfico y dispositivos de red, para la detección oportuna de amenazas que puedan explotar vulnerabilidades de los activos de información en la Dependencia o Entidad.

Implementar un mecanismo de revisión constante de la reputación del segmento de IP, en caso de estar en lista negra, identificar la(s) causa(s) por la(s) que la reputación del segmento decreció, solucionar el problema y solicitar la exclusión de la lista negra.

Implementar uso de protocolos seguros HTTPS, SFTP y SSH, en lugar de HTTP, FTP y Telnet. Priorizar el uso de *Let's Encrypt* e implementar Autoridades de Certificación internas de confianza.

Restringir el acceso a invitados a una red sólo con salida a internet, que no tenga acceso a la red interna de la Dependencia o Entidad, estableciendo el tiempo máximo de autorización de los dispositivos.

En caso de contar con proveedores, el personal interno de la Dependencia o Entidad deberá tener acceso a los equipos de telecomunicaciones, además de estos, con usuarios y con privilegios de lectura o monitoreo a los equipos de telecomunicaciones, que deberán estar autorizados y documentados.

Equipo de cómputo

Crear las imágenes de instalación base con las aplicaciones permitidas al interior de cada Dependencia o Entidad, de preferencia conformadas por software libre; configuración de los sistemas operativos y habilitación de los usuarios estrictamente necesarios de acuerdo con el grupo o rol de la persona servidora pública y priorizando el principio de menor privilegio.

Establecer los procedimientos necesarios para la autorización, el ingreso, registro y la conexión de equipos de cómputo personales a las redes institucionales.

Implementar herramientas de monitoreo de aplicaciones instaladas y actividad no deseada en los equipos de cómputo.

Aplicar medidas necesarias para detectar y evitar la desinstalación o deshabilitación de las herramientas o los servicios de seguridad aplicados en la Dependencia o Entidad.

Aplicar borrado seguro o destrucción de equipos que dejan de ser útiles para la Dependencia o Entidad y mantener evidencia auditable del proceso.

Instalar y actualizar software antimalware en los equipos de escritorio, portátiles y servidores para evitar la instalación, propagación y ejecución de malware en diversos puntos de la red interna de la Dependencia o Entidad.

Realizar el fortalecimiento de seguridad en los servidores, aplicando las configuraciones recomendadas. Se deberán cerrar puertos y deshabilitar servicios que no se utilicen.

Implementar un mecanismo de aplicación de parches de seguridad indicados por los fabricantes de hardware y software.

Habilitar políticas de permisos de grupo para restringir el uso de herramientas de línea de comando (Powershell, Terminal, Shell) a cualquier usuario.

Habilitar y configurar el firewall de cada equipo terminal para bloquear todo el tráfico entrante, permitiendo sólo el tráfico autorizado. Únicamente podrá deshabilitar el firewall la persona servidora pública facultada y con la autorización correspondiente.

Los Firewalls de cada servidor deben estar activados y configurados de acuerdo con las necesidades del servicio requerido en todo momento y no podrá permanecer deshabilitado; únicamente se podrá deshabilitar con autorización y toma de responsabilidad por la persona servidora pública facultada.

Registrar, monitorear y analizar los eventos de seguridad de los equipos de cómputo, dispositivos de red, servidores, aplicaciones institucionales y otro software o activo de información que se considere importante para la Dependencia o Entidad, que ayude a detectar posibles incidentes de seguridad.

En caso de contar con proveedor, el personal interno de la Dependencia o Entidad deberá tener acceso a los equipos de cómputo, además del proveedor, incluyendo accesos , y estos deberán estar autorizados y documentados.

Tecnología Móvil
Establecer los procedimientos necesarios para la autorización, el ingreso, registro y la conexión de dispositivos móviles personales a las redes institucionales. En caso de requerirse que los dispositivos móviles, propiedad de terceros, accedan a la red o interactúen con los dispositivos conectados a la infraestructura de la Dependencia o Entidad, éstos deberán contar con autorización previa y tener acceso a redes diferenciadas; sólo deberá conectarse a la red como invitado con acceso a internet y no podrá conectarse a los servicios internos de la Dependencia o Entidad. Instalar mecanismos de cifrado de datos en los dispositivos electrónicos portátiles que contengan información de la Dependencia o Entidad.
Sistemas, aplicaciones y servicios
Crear y actualizar el inventario de aplicaciones y sistemas de información en la Dependencia o Entidad. Implementar un repositorio del código fuente Institucional, este deberá estar bajo control y administración de la Dependencia o Entidad e independiente a los contratos con fábricas de software. Mantener bitácoras y registros con fines de auditoría y trazabilidad de procesos de desarrollo de software.

Los sistemas esenciales deben estar separados de la red de datos interna y sólo se les deberá permitir el acceso o salida directa hacia la Internet, como mínimo, con una protección perimetral de red.

Para las aplicaciones o servicios que estén expuestos en Internet y que manejen información sensible, como Información confidencial o reservada, datos personales y datos personales sensibles, la comunicación deberá ser cifrada a fin de evitar que ésta sea modificada o expuesta a personas no autorizadas.

El desarrollo de sistemas o aplicaciones deberá regirse bajo los principios de privilegio mínimo y funcionalidad mínima, validando cada operación que realiza el usuario a través de verificación explícita, todas las entradas, incluido el tamaño, el tipo de datos, los rangos o formatos aceptables y los posibles errores.

Los ambientes de desarrollo y pruebas deberán estar separados entre ellos y de ambientes productivos, se deberán seguir las medidas de seguridad que se implementan para un ambiente de producción con la finalidad de simular y validar los escenarios que expongan riesgos de seguridad.

El responsable del desarrollo deberá establecer los controles necesarios, así como los criterios y el perfil del usuario que tendrá acceso al código fuente para realizar cambios e implementaciones que requiera el sistema o aplicación, en horarios no hábiles para no afectar la disponibilidad del servicio.

Actualizar las bibliotecas y lenguajes de programación utilizados en el desarrollo de aplicaciones y sistemas para minimizar la exposición a vulnerabilidades, en caso de que dicha actualización afecte la funcionalidad o desempeño del sistema y/o aplicativo, se deberá planificar y realizar la adecuación a los mismos.

Realizar pruebas unitarias y de integridad a los sistemas desarrollados.

Realizar pruebas de estrés y carga masiva de datos a los sistemas y aplicaciones desarrollados antes de su implementación en ambientes productivos.

Realizar un análisis de vulnerabilidades a los sistemas o aplicaciones, en particular las identificadas como esenciales para la Dependencia o Entidad, para verificar que cumplan con los requisitos mínimos previo a su operación en producción.

Realizar pruebas de respaldo y restauración de los sistemas, aplicaciones y los servicios y de la información u otros activos de información relacionados con estos.

Para el servicio de correo electrónico, configurar adecuadamente el marco de políticas del remitente (SPF), el correo identificado de llaves de dominio (DKIM) y la autenticación, informes y conformidad de mensajes basados en el dominio (DMARC), estos ayudarán a autenticar a los remitentes mediante el dominio específico de una Dependencia o Entidad. SPF evitará que personas malintencionadas envíen correos electrónicos en nombre del dominio de una Dependencia o Entidad.

Además de SPF, DKIM verificará si el propietario de ese dominio realmente envió un correo electrónico. DMARC utiliza tanto SPF como DKIM para determinar la autenticidad del contenido de un mensaje de correo electrónico.

Proteger los datos personales que son utilizados por las aplicaciones web y móviles contra posibles amenazas, reforzando el cumplimiento del presente y de la Ley general de protección de datos personales.

Supervisar el efectivo cumplimiento de las actividades y acuerdos efectuados con proveedores de los bienes y servicios, que por falta u omisión de estas, puedan incidir en eventos o incidentes de seguridad y afectar negativamente a la Dependencia o Entidad.

Bases de datos
Establecer un mecanismo para realizar pruebas de respaldo y restauración de las bases de datos institucionales. Es recomendable que los respaldos de estas bases de datos también se encuentren cifrados.

Definir usuarios, roles y permisos específicos para las diferentes operaciones en las bases de datos.

Definir el inventario de todas las bases de datos institucionales y su interoperabilidad con otros sistemas internos o externos y con otras Instituciones públicas.

Ofuscar información de bases de datos que sean utilizadas en ambientes de desarrollo.

Utilizar cifrado en reposo y en tránsito, cuando la base de datos contenga datos personales.

En bases de datos que contengan información confidencial, el contenido de las tuplas debe ir cifrado utilizando llaves cuya posesión sea exclusivamente para personas autorizadas y nunca tengan acceso el administrador del sistema operativo ni el DBA.