República de Panamá

AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL

Resolución No. 13
13 de marzo de 2018

"Por la cual se aprueba el documento titulado: **ESTÁNDARES PARA LA SEGURIDAD DE LA INFORMACIÓN Y LAS TIC".**

El Administrador General de la Autoridad Nacional para la Innovación Gubernamental, en uso de sus facultades legales, y

CONSIDERANDO:

Que mediante la Ley 65 de 30 de octubre de 2009, se creó la Autoridad Nacional para la Innovación Gubernamental, en adelante la AIG, como una entidad con personería jurídica, patrimonio propio y autonomía en su régimen interno, con capacidad de adquirir derechos y contraer obligaciones, administrar sus bienes y gestionar sus recursos, con competencia para planificar, coordinar, emitir directrices, supervisar, colaborar, apoyar y promover el uso óptimo de las tecnologías de la información y comunicaciones en el sector gubernamental, para la modernización de la gestión pública.

Que de conformidad con el artículo 3, numeral 11 de la Ley 65 de 30 de octubre de 2009, es facultad de la AIG emitir directrices para establecer los estándares necesarios para el desarrollo y la protección de los sistemas tecnológicos del Estado y velar por su cumplimiento.

Que el artículo 3 del Decreto Ejecutivo No. 205 de 9 de marzo de 2010, dispone que para el ejercicio de sus funciones, la AIG emitirá criterios e impartirá instrucciones mediante circulares y resoluciones a las entidades gubernamentales, concernientes a estándares de diseño, desarrollo, operación y protección de sistemas y equipos tecnológicos de la información y telecomunicaciones de las entidades del Estado.

Que el Decreto Ejecutivo No. 826 de 11 de agosto de 2010 "Que Aprueba la Estructura Organizacional de la Autoridad Nacional para la Innovación Gubernamental" establece que la Dirección de Arquitectura Tecnológica tiene entre sus objetivos desarrollar los estándares y directrices tecnológicas que deberán cumplir las instituciones del Estado, en cumplimiento de la Ley 65 de 30 de octubre de 2009.

Que en ejercicio de sus facultades legales, la AIG ha considerado necesario adoptar el documento titulado **"ESTÁNDARES PARA LA SEGURIDAD DE LA INFORMACIÓN Y LAS TIC"**, que tiene como objetivo principal el conocimiento y referencia de las entidades estatales de las normas emitidas para la seguridad y protección de la información, así como disponer de los controles y programas requeridos para la protección de la confidencialidad, integridad y disponibilidad de la información, acorde a la naturaleza y segmento aplicable a los datos, por lo que el suscrito,

RESUELVE:

PRIMERO: Aprobar el documento titulado: **"ESTÁNDARES PARA LA SEGURIDAD DE LA INFORMACIÓN Y LAS TIC"**, tal cual se adjunta a la presente Resolución.

ASESORIA LEGAL VISADO AIG

SEGUNDO: La Autoridad Nacional para la Innovación Gubernamental (AIG) por conducto de la Dirección de Arquitectura Tecnológica, será la responsable de promover, inspeccionar y controlar el cumplimiento de **ESTÁNDARES PARA LA SEGURIDAD DE LA INFORMACIÓN Y LAS TIC,** en las instituciones del Estado.

TERCERO: Ordenar la publicación de la presente Resolución en Gaceta Oficial.

CUARTO: Esta Resolución regirá a partir de su publicación.

FUNDAMENTO DE DERECHO: Ley 65 de 20 de octubre de 2009, Ley 83 de 9 de noviembre de 2012 y Decreto Ejecutivo 205 de 9 de marzo de 2010, Decreto Ejecutivo No. 826 de 11 de agosto de 2010.

PUBLÍQUESE Y CÚMPLASE,

IRVIN A. HALMAN
ADMINISTRADOR GENERAL

IAH/AB/TB/jvm

IAH/GR/TB/jvm

ASESORÍA LEGAL
REVISADO
AIG

Este documento es fiel copia del original, que reposa en custodia de la Oficina de Asesoría Legal de la Autoridad Nacional para la Innovación Gubernamental.

Oficina de Asesoría Legal

Estándares para la Seguridad de la Información y las TIC.

Un documento para salvaguardar la información del Estado

Autoridad Nacional para la Innovación Gubernamental

Estándares y Normas
Septiembre 2017
Versión 0.0

AUTORIDAD NACIONAL PARA LA INNOVACION GUBERNAMENTAL
Título: **Estándares para la Seguridad de la Información y las TIC**
Realizado por: **Ing. Anabel Broce de Tapia** **Directora de Arquitectura Tecnológica**
Autorizado por: **Ing. Irvin A. Halman** **Administrador General**

Control de Cambios	
Número de Versión	Fecha de Revisión: septiembre 2017 Fecha de Vigencia: actual
Versión 0.0	Confeccionaron el documento: Anabel Broce de Tapia, AIG Abdiel Vergara, AIG Colaboración: Demóstenes García, IFARHU

Revisado por:

IRVIN A. HALMAN
Administrador General

LUIS FASANO
Sub Administrador General

ANABEL BROCE DE TAPIA
Directora de Arquitectura Tecnológica
CARLOS DIAZ
Datos Abiertos
DIONYS SÁNCHEZ
Dirección de Tecnología y Transformación
SAMUEL DIAZ
Dirección de Innovación
GABRIEL REYES
Gobernanza TI
GISELA GONZÁLEZ
Jefa de la Oficina de Auditoría Interna
TERESA BERBEY
Legal

SILVIA BATISTA
ERIC ESPINO
JULIO PRESTAN
NADDIEE ATENCIO

CONTENIDO

INTRODUCCIÓN

Las entidades gubernamentales requieren mantener sus sistemas disponibles, con comunicación, poder identificar problemas, realizar análisis de riesgos, mantener la integridad de los sistemas de información, confidencialidad y realizar la recuperación de los riesgos.

La seguridad de la información tiene un impacto respecto a la privacidad, dependiendo de la naturaleza de confidencialidad, valor y sensibilidad de los datos administrados, gestionados por las entidades y entre entidades para la interoperabilidad.

Esto puede agravarse debido a que la información puede ser divulgada, mal utilizada, robada, borrada o saboteada afectando su disponibilidad, al ciudadano y poniendo en riesgo al país.

Por tanto, las entidades gubernamentales requieren mantener sus sistemas disponibles y con capacidad de identificar, analizar y atender riesgos, vulnerabilidades o amenazas informáticas, mantener la integridad de su información, confidencialidad y realizar la recuperación de los incidentes.

El presente documento contiene las principales normas generales de cumplimiento para el debido resguardo de la información aplicando normas de seguridad y protección de la información, que tiene como objeto mantener la confidencialidad, integridad y disponibilidad de la información contenida en los archivos, bases de datos, documentos, equipos y medios de almacenamiento; asegurando la continuidad del negocio, protección de los datos almacenado, mediante procesos, herramientas y protocolos aplicables al acceso, uso, divulgación, interrupción y destrucción no autorizada sobre la información crítica, sensible o de valor.

La información se considera

Crítica: cuando es indispensable para la operación de la entidad.
De valor: cuando es un activo importante de la entidad.
Sensible: cuando debe ser conocida por las personas autorizadas, así como para un uso específico para el cual está siendo gestionada.

Los estándares y niveles de seguridad de la información deben ser cónsonos con la naturaleza de la información, tales como la de los sectores de salud, seguridad, logística, financiera, registral, tributaria, fiscal, electoral, entre otros.

OBJETIVOS

Presentar para el conocimiento y referencia de las entidades las normas pertinentes a la seguridad y protección de la información que deben implementarse.

Disponer de los controles y programas requeridos para la protección de la confidencialidad, integridad y disponibilidad de la información, acorde a la naturaleza y segmento aplicable a los datos.

AMBITO DE APLICACIÓN

El presente documento será aplicado por todas las entidades del Estado, bajo responsabilidad de las direcciones de informática. La implementación de este estándar puede ser progresiva y de acuerdo con el nivel de riesgo de la entidad.

La presente norma es aplicable a todas las entidades del Estado y las sociedades anónimas en las que el Estado sea propietario del cincuenta y uno por ciento (51%) o más de sus acciones del patrimonio de la República de Panamá.

Esta norma debe ser del cumplimiento del Órgano Legislativo, el Órgano Ejecutivo (Gobierno Central, Entidades Autónomas y Semiautónomas, Empresas Publicas, los Intermediarios Financieros), el Órgano Judicial, Patronatos regentes de instituciones públicas o bienes públicos, el Régimen Municipal (en las áreas que aplique según el ente que administre el tema de tecnología), se exceptúan aquellos casos en que leyes especiales disponga otro régimen.

Es obligación de todo Gerente, Director o Jefe de la Oficina de Tecnología, el cumplimiento de la Norma y su difusión a los miembros de la entidad que regenten.

BASE LEGAL

Ley 65 de 30 de octubre de 2009, "Que crea la Autoridad Nacional para la Innovación Gubernamental".

Decreto Ejecutivo No. 205 de 9 de marzo de 2010 "Por la cual se Reglamenta la Ley 65 de 30 de octubre de 2009 "Que crea la Autoridad Nacional para la Innovación Gubernamental ".

Decreto Ejecutivo No. 826 de 11 de agosto de 2010, Que Aprueba la Estructura Organizativa de la Autoridad Nacional para la Innovación Gubernamental.

Artículo 29 de la Constitución Política de la República de Panamá, sobre la inviolabilidad de la correspondencia y documentos privados.

GLOSARIO

Acceso a la información: permiso otorgado para poder ver la información alojada en los repositorios de la entidad.

Activos de información: datos o información que tienen valor para una entidad gubernamental.

Activo de la información: elemento que contiene o manipula información. Son archivos y bases de datos, documentos, contratos, acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, sensores, dispositivos, maquinarias, incluyendo a las personas, que son las que generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información.

Alerta: vulnerabilidad o amenaza que pueda afectar a la información.

Amenaza: causa potencial de un incidente indeseado que puede dar lugar a la perdida de la seguridad de la información.

Análisis de riesgo: método cualitativo o cuantitativo para la evaluación del impacto del riesgo en la toma de decisiones.

Antivirus: software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus.

Arquitectura tecnológica: estructura de hardware, software y redes requerida para dar soporte a la implementación de los aplicativos de cómputo, soluciones tecnológicas o servicios de TIC de la Institución.

Autenticación: proceso de confirmación de la identidad del usuario dentro de las áreas restringidas y sistemas utilizados.

Confidencialidad: proceso de asegurar que la información solo sea conocida por los usuarios autorizados.

Contraseña: conjunto de letras, números y símbolos, o incluso frases, utilizadas para autenticar usuarios en un sistema informático. Para que el uso de contraseñas sea efectivo es necesario escogerlas de manera que sean difíciles de adivinar para un atacante.

Control: procesos para mitigar y evitar los riesgos.

Correo electrónico: servicio de mensajería en red que permite el intercambio de mensajes, a través de sistemas de comunicación electrónicos.

Cortafuegos (firewall): aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno.

Criptografía: técnica de cifrado o codificado destinada a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Denegación de Servicio Distribuido (DDoS): ataque en el cual determinados recursos de una computadora o red se hacen inaccesibles por su saturación.

Disponibilidad: habilidad de la comunidad de usuarios para acceder al sistema, someter nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos.

Dispositivos Móviles: computadoras de mano de tamaño pequeño, con capacidad de procesamiento, memoria y conexión a internet.

Estándares de Seguridad: conjunto de normas que deben seguir las entidades del gobierno para salvaguardar la información con el buen manejo de las TIC´s.

Firewalls XML: dispositivo desarrollaron específicamente para filtrar y prevenir ataques por medio de transacciones XML que entran y salen por la red de una institución.

Hardware: partes físicas o tangibles de un sistema de información.

Infraestructuras críticas: instalaciones, redes, servicios y equipos asociados o vinculados con activos de TIC o activos de información, cuya afectación, interrupción o destrucción tendría un impacto mayor, entre otros, en la salud, la seguridad, el bienestar económico de la población o en el eficaz funcionamiento de las Instituciones.

Información: conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento de un usuario o sistema.

Integridad: propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada, para salvaguardar la precisión y completitud de los recursos.

Interoperabilidad: es la capacidad que tiene un sistema de información para intercambiar datos con otros sistemas con la capacidad de procesarlos.

Ipsec: conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

Malware: descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse.

Seguridad de la información: capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.

Ransomware: tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.

Riesgo: materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio.

Seguridad: conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Ambos son tomados en cuenta al momento de establecer la seguridad de la Información debido a que podrían ser causa de la pérdida de credibilidad, pérdida de negocios, demandas legales o incluso la quiebra o huelga nacional.

Sistema de prevención y detección de intrusos: dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Software: componentes lógicos o intangibles de un sistema de información, tales como programas, aplicaciones, sistemas operativos, entre otros. Telecomunicaciones.

Software Malicioso: conocido como malware, contiene virus, spyware y otros programas indeseados que se instalan en su computadora, teléfono o aparato móvil sin su consentimiento. Estos programas pueden colapsar el funcionamiento de su equipo para monitorear y controlar su actividad en Internet.

Spyware: paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo.

SQL Injection (inyección SQL): método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos.

Token: dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

Troyano: tipo de malware que se hace pasar por una aplicación inofensiva pero en realidad crea una puerta trasera que permite la administración del sistema del usuario por parte del atacante.

Usuario: entidad o individuo que utiliza el sistema.

Validación: actividad que asegura que un servicio de TIC, producto o entregable, nuevo o modificado, satisface las necesidades acordadas previamente con la unidad administrativa solicitante.

Verificación: actividad que permite revisar si un servicio de TIC o cualquier otro producto o entregable, está completo y acorde con su especificación de diseño.

Virus: programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:

- Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.
- Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Vulnerabilidades: debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a la infraestructura crítica, así como a los activos de información.

WAF: protege el acceso a las aplicaciones web alojadas dentro y fuera de su red, analizando el tráfico tanto entrante como saliente.

ESTANDAR PARA LA SEGURIDAD DE LA INFORMACIÓN Y LAS TIC

Estas reglas de referencia sobre la Seguridad de la información se basan en normas ISO/IEC, OWASP, W3C, NIST, Web Services Security y documentos de referencia expuestos en la Bibliografía.
Las entidades gubernamentales van a interoperar por razones diferentes y con niveles de riesgo diferente para la información que van a compartir. Sabemos que van a tener diferentes niveles técnicos del personal encargado y capacidades financieras diferentes para invertir. Hemos definido 3 categorías y para cada una de ellas especificaremos los requerimientos mínimos con base en su nivel.

- **Nivel básico:** Las entidades utilizan la información compartida únicamente para sus procesos internos. La información compartida no se utilizará como base para publicaciones al público en general y los datos que la componen no incluyen datos privados sobre la identidad de las personas o datos que pudieran considerarse sensitivos.

- **Nivel intermedio:** La información que comparten las entidades sirve como base para publicaciones que serán divulgadas al público en general. Para un atacante puede ser atractivo alterar el contenido por el impacto que esto representa. Esta información que se comparte no contiene datos privados sobre la identidad de las personas u otros datos que pudieran considerarse sensitivos.

- **Nivel sensitivo:** La información que se comparte contiene datos privados de identidad de las personas o información que pudiera considerarse sensitiva. Otra posibilidad es que la información compartida se integre a un cuerpo de datos que será divulgado públicamente.

Requerimiento de seguridad	Nivel Básico	Nivel Intermedio	Nivel Sensitivo
Ambas entidades deben tener configurado un Firewall con reglas que protejan de	Opcional, puede ser el Firewall de la red.	Requerido, puede ser el Firewall de la red.	Requerido, debe ser un firewall diferente al de la red interna.

accesos no autorizados a los datos y a las redes de las respectivas entidades.			
Implementar autenticación a nivel del servicio al menos por validación de usuario y contraseña.	Requerido	Opcional	Opcional
Implementar autenticación a nivel del servicio por medio de certificado digital.	Opcional	Requerido	Requerido
Los servicios web deben implementar mejores prácticas de seguridad según la especificación de "**NIST 800-95** Guide to secure web services" o "OASIS Web Services Security: **SOAP Message Security 1.1**".	Opcional	Requerido	Requerido
Las entidades que están interoperando no deben permitir el acceso de forma directa a sus bases de datos (por ejemplo por medio de SQL) ni divulgar la estructura de la misma. El servicio web se encargará del acopio de la solicitud y la entrega de los resultados en el formato que acuerden las entidades.	Requerido	Requerido	Requerido
Los servidores involucrados en el intercambio de información deben cumplir con lo especificado en el documento: "**NIST SP 800-123** Guide to general server security".	Requerido	Requerido	Requerido
Implementar un sistema de correlación de eventos.	Opcional	Opcional	Requerido
Se debe implementar el protocolo IP-SEC entre los equipos de las entidades que van a compartir información.	Opcional	Opcional	Requerido
Implementar un sistema de prevención de intrusos. (IPS)	Opcional	Opcional	Opcional
Implementar un firewall	Opcional	Opcional	Opcional

XML/JSON			

1. ORGANIZACIÓN INTERNA

- **La información** es considerada como un **activo del Estado**. La entidad es responsable por sus activos de información (como: bases de datos, archivos, información, datos, códigos fuentes, claves, llaves, entre otros) sistemas informáticos, hardware, redes y comunicaciones; debe establecer las funciones y responsabilidades en materia de seguridad de la información y cumplir con los estándares establecidos por la Autoridad Nacional para la Innovación Gubernamental.
- **Los funcionarios** de la entidad deberán custodiar, mantener, conservar, monitorear, asegurar y rendir cuentas por los activos de información, software, hardware y demás componentes informáticos a su cargo, cumpliendo con las funciones asignadas, que deberán ser creadas con deberes y permisos que eviten el conflicto de interés y actividades inapropiadas. No deberá haber contacto, en materia de seguridad de la información, con las autoridades o individuos internos y/o externos, a fin de garantizar la independencia en la preservación, integridad, seguridad, confidencialidad, disponibilidad y la privacidad de la información.
- Las entidades gubernamentales, de acuerdo con la facilidad de recursos de personal con el que cuenten, establecerán un **modelo de Seguridad** de la Información, designando al responsable de la seguridad de la información de la Entidad y la constitución de un grupo estratégico de la Seguridad de la Información, que serán responsables de salvaguardar los activos de la información de la Entidad, creando los lineamientos, guías o reglamentaciones y procedimientos de seguridad para la institución, los cuales deberán ser diseñados implementados, documentados, monitoreados a fin de validar su cumplimiento. Además deberán fomentar la aplicación de las políticas de seguridad, concientizar y capacitar a los usuarios.
- El cumplimiento de los estándares y procedimientos de seguridad implementados en una entidad gubernamental **son obligatorios**; si un individuo u área incurre en alguna violación, por negligencia o intencionalmente, se deberán tomar las medidas correspondientes.
- La entidad gubernamental debe **verificar periódicamente el cumplimiento** de los estándares y procedimientos de seguridad de la información establecidos.
- La entidad gubernamental debe facilitar **la divulgación** de los estándares y procedimientos de seguridad de la información a todos sus colaboradores.
- La entidad gubernamental debe promover activamente la **cultura de seguridad** de la información.

- La entidad debe **diseñar y documentar los procesos** y procedimientos establecidos para lograr ejecutar los estándares de seguridad, especialmente para cada una de las secciones de este estándar.
- **La entidad debe garantizar**, de manera razonable, la **confidencialidad,** integridad y disponibilidad de la información, lo que implica protegerla contra el uso, divulgación o modificación no autorizados, daño o pérdidas u otros factores.
- La entidad debe implementar un conjunto de **normas y reglamentos internos de seguridad** de la información.
- **El personal de la entidad debe conocer** y estar comprometido con las regulaciones sobre la seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.
- La entidad debe **proteger los recursos** estableciendo un ambiente físico, eficiente, seguro y controlado, con medidas de protección fundamentadas en políticas vigentes y de análisis de riesgo.
- La entidad debe implementar las medidas de seguridad relacionadas con la **operación de los recursos y las comunicaciones**, minimizar su riesgo de fallas y proteger la integridad de la información.
- La entidad debe proteger la información con uso de accesos restringido para **usuarios no autorizados**.
- Se debe mantener los procesos de implementación y **mantenimiento de infraestructuras tecnológicas** y a fin de evitar el acceso no autorizado, daño o pérdida de información.
- La entidad tiene la responsabilidad de incluir dentro del **plan anual de auditorías internas y externas** de verificación aleatoria a los equipos de cómputo de todas las dependencias y puntos de atención de la entidad.
- La **instalación, reparación o retiro de cualquier componente de hardware o software** de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por los funcionarios de la entidad, o personal de terceras partes autorizados. **Destruir la información de los equipos dañados que entren al proceso de descarte**.
- Los equipos de cómputo deben ser **transportados** con las medidas de seguridad apropiadas, que garanticen su integridad física.
- La entidad debe proveer los recursos necesarios para la implantación de controles que permitan la **separación de ambientes de desarrollo, control de versiones del código fuente, prueba, preproducción y producción**, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo, prueba, pre producción y producción.

2. LA GESTIÓN DE ACTIVOS

- Ninguna persona puede reclamar **derechos de propiedad intelectual** sobre un activo de información del Estado. Todos los activos de información deberán ser **gestionados y monitoreados por la entidad responsable de generarlos** y deberán ser **inventariados e identificados** colocando los responsables de seguridad del activo.
- Se deben definir las normas de uso aceptable y en los casos que el responsable del activo de la información, **termina la relación laboral o suspende su labor**, los activos informáticos deben ser formalmente entregados al personal asignado por la entidad, deshabilitándole de forma automática todo acceso a la información.
- La información, datos, información **que fluye a través de medios** de trasmisión o cableado, archivos físicos, base de datos, sistemas, servicios y los equipos propiedad del estado (computadoras, celulares, equipos de comunicación como: routers, switch, centrales telefónicas, cámaras, unidades de almacenamiento, aplicaciones o software, códigos fuentes, documentos como: contratos, procedimientos, planes, registros, entre otros), son activos de las entidades del estado y se proporcionan a los funcionarios y terceros autorizados sólo para cumplir con los propósitos de la entidad, manteniendo un inventario, clasificación y etiquetado, asegurando un nivel adecuado para la protección sobre ellos.
- La información debe **ser clasificada y etiquetada** por sus propietarios, según la importancia, valor, nivel de seguridad, protección y manejo requerido, pudiendo clasificar las que tengan carácter de infraestructura Crítica de Seguridad Nacional o activos estratégicos o esencial.
- La entidad debe realizar la **configuración inicial correcta** de los recursos tecnológicos para preservar la seguridad de la información.
- Se debe realizar **revisiones periódicas de los recursos** de los sistemas de información de la entidad.
- La entidad debe implantar los controles que **regulen el uso** de periféricos y medios de almacenamiento en la plataforma tecnológica.
- La entidad debe asegurar que los **usuarios o perfiles de usuarios correctos** tengan acceso de los recursos tecnológicos y sistemas de información.
- La entidad debe **proveer los mecanismos y estrategias** necesarias para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos dentro y fuera de las instalaciones de las instituciones públicas con las configuraciones seguras.
- La entidad debe asegurarse de que los datos que son procesados mediante el IT corresponden a **transacciones válidas y debidamente autorizadas**, que son procesados en forma completa, exacta, oportuna, transmitidos y almacenados en forma íntegra y desechados en forma segura (eliminada la información completamente antes de desecharla), mediante el monitoreo realizado por funcionarios públicos.

- **Los Medios de almacenamiento** de la información deberán ser mantenidos, administrados, manejados, controlados, movidos, transportados y eliminados de manera tal que el contenido de la información no se vea comprometida.
- Las **Bases de Datos** deben ser administradas, monitoreadas, controladas por **Administradores de base de datos**.
- Se debe establecer **lineamientos para el manejo y eliminación seguro** de los medios de almacenamientos.

3. SEGURIDAD FÍSICA Y AMBIENTAL

- Definir el **perímetro y barreras físicas** del Centro de Cómputo, áreas relacionadas y la entidad, con controles y procedimientos de entrada o acceso, protección del local, oficinas, salas, zonas de entrega, atención al usuario *y otros*, contra el acceso no autorizado.
- Se debe tener **sistemas de control ambiental** de temperatura y humedad, sistemas de detección y extinción de incendios especiales para centros de cómputo, sistemas de descarga eléctrica, sistemas de vigilancia, monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- Se debe efectuar **prevención y protección** contra incendios, inundaciones, fluctuaciones de voltaje (reguladores, circuito separado con conexión a tierra) y eventos fortuitos como terremotos, dispositivos explosivos, descargas eléctricas (rayos), como una de las primeras acciones que se deben implementar.
- Los equipos y **cableados** deben estar bien sujetos, organizados, etiquetados y protegidos.
- Los equipos informáticos no deben ser **trasladados** fuera de las instalaciones o entre departamentos o usuarios a menos que sea autorizado y deben ser protegidos adecuadamente, tanto dentro, como fuera de las instalaciones. Debe detallarse en el proceso o instructivos quien debe autorizar el movimiento o traslado de los equipos.
- **Mantener los activos** de información en área cerrada, en mobiliario con cerradura, caja de seguridad o equivalente, pudiendo cumplir con estándares IP o estándares NEMA. Si son equipos o servidores, generalmente generan calor en gran magnitud por lo que el área debe tener aire acondicionado de precisión que evite el mal funcionamiento y el daño tanto en el equipo como al personal.
- Abstenerse de efectuar **reproducciones** totales o parciales de la información que manipula, genera o recibe, sin la previa autorización de la Institución o entidad.
- Antes que los **medios de almacenamiento sean retirados o reutilizados,** la información, debe ser eliminada, efectuando la eliminación total de cualquier dato almacenado en medios de almacenamiento, por el método indicado por la

Institución. Los equipos desatendidos se deben asegurar.

4. CONTROL DE ACCESO, USO Y CONEXIONES

- Los **accesos a los activos de información**, aplicaciones, servidores, conexiones físicas o lógicas, equipos y dispositivos de comunicaciones, servicios de intercambio de información (webservice), bases de datos, archivos, equipos tecnológicos u otros equipos, sensores o dispositivos inteligentes (Smart) y medios electrónicos que contengan información sensitiva deben ser restringidos, asignando niveles de seguridad de acuerdo con las funciones o roles o actividades asignadas a los usuarios; limitando sus derechos de acceso, asignando permisos mínimos y sin utilizar el usuario administrador para accesos desde la aplicación.
- Se deberán gestionar las contraseñas, manteniendo revisiones periódicas y efectuando actualizaciones inmediatas, al darse cambios en las **actividades o funciones del usuario**.
- Se deben definir las normas de acceso y en los casos que el responsable del activo de la información, **termina la relación laboral o suspende su labor**, se debe deshabilitar de forma automática todo acceso a la información.
- **Los usuarios deben ser conscientes** de su responsabilidad para mantener un control y actualización eficaz y confidencial de sus contraseñas de acceso, información y demás componentes relacionados, aplicando una cultura de trabajo orientada a la protección de la información, dando a conocer cualquier evento, incidente o problema que se detecte.
- El **acceso a la información por parte del personal externo** a la institución debe ser de forma restringida, exceptuando las consultas a datos públicos; el personal externo solo podrá ingresar por medio de un Portal seguro o pantalla, con niveles de permiso en el acceso, de acuerdo con las normas de Control de Acceso creadas por la institución y aplicando la administración de contraseñas, con el respectivo monitoreo con control de las actividades y los respectivos permisos.
- El **acceso físico o lógico** debe estar plenamente justificado, especificando las fechas y horarios en que los accesos son permitidos, previamente acordados y registrado por el responsable de la entidad. El proceso de acceso se debe contemplar mediante un contrato con el proveedor.
- Se debe aplicar acceso restringido al **código fuente del programa**, llevando el control de las modificaciones, especificando el periodo en que se realizaron las modificaciones, el o los usuarios que las realizaron, el o los usuarios que realizaron las pruebas, manteniendo un registro de las versiones y cada modificación que se incluya a dicha versión. Se debe mantener un procedimiento

de registro y control muy claro de los cambios realizados y la implementación o colocación de dichos cambios entre los ambientes de desarrollo, prueba y producción.

- Todas los funcionarios con acceso a **información confidencial** o de acceso restringido o privilegiada y todos los proveedores con acceso a datos o información deben firmar una carta, contrato o acuerdo de confidencialidad en el que aceptan que los datos e información es un activo privado y propiedad del Estado, se obligan a proteger contra cualquier acto que pueda atentar contra su confidencialidad, integridad, seguridad y disponibilidad, aún después de terminar su relación de trabajo con la entidad, evitando su uso indebido, no autorizado, beneficio propio o externo y aceptan cumplir con este estándar de seguridad de acuerdo al tipo de información que maneja el sistema o plataforma.
- Se debe mantener la seguridad, monitoreo y el control de los **accesos de los proveedores y funcionarios** a la información, datos, equipos y componentes de comunicaciones, bases de datos, aplicaciones y demás servicios relacionados, manteniendo los accesos en una bitácora detallada con una retención de la misma al menos de un (1) año.
- Los funcionarios de la entidad y el personal externo deben **bloquear sus estaciones de trabajo** en el momento de abandonar su puesto de trabajo. Este bloqueo se recomienda sea automático y su configuración solo podrá ser modificada por el usuario administrador.
- **Las sesiones activas** deben ser cerradas en los equipos cuando se finalice la función realizada en el sistema de información. Se recomienda que la acción de cerrado sea automática.

Conexiones Remotas

- Se debe implementar **procedimientos y controles** de seguridad para establecer conexiones remotas.
- Se debe restringir las conexiones remotas a los recursos y a la información. En donde solo los usuarios con acceso autorizado podrán realizar estas conexiones.
- Se recomienda implementar políticas que prohíban la **instalación de programas** de control remoto sin el conocimiento explícito del departamento de Tecnología. En el Departamento de Tecnología deben existir funcionarios autorizados con usuarios administradores que lleven la función de restringir los accesos a descargar software y demás programas para garantizar la seguridad de los equipos y de la información. Si se permite el acceso como administrador de la maquina a funcionarios ajenos a este departamento se debe llevar el control, monitoreo y revisión de las maquinas.
- Se debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos e información.
- Se debe implementar, administrar y mantener de manera segura la prestación del **servicio de Internet utilizando perfiles de acceso** para los usuarios.

- La entidad debe monitorear constantemente el **servicio de Internet**, la calidad y accesos no autorizados.
- Se debe establecer controles para identificar y evitar la **descarga de software** no autorizado.
- Se debe prohibir almacenar información sensible, confidencial o privilegiada en sitios de almacenamiento en **nubes públicas**.
- Se recomienda restringir el uso de **memorias USB**, sobre todo en dispositivos de almacenamiento de información importante o sensitiva, mediante la creación de una política de uso y la desactivación de los puertos USB en todos los equipos de la institución. Las excepciones al uso de estos dispositivos deberán estar debidamente justificados.
- La entidad debe generar registros de navegación y los accesos de los usuarios **al Internet**.
- Se debe bloquear el acceso a páginas que atenten contra la moral de las personas o las normas establecidas por la entidad.
- La entidad debe crear, modificar, bloquear o eliminar **cuentas de usuarios** sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.
- Se deben definir los lineamientos para la **configuración de contraseñas** que aplicaran sobre cada plataforma tecnológica, los servicios de red y los sistemas de información, dichos lineamientos deben considerar aspectos como longitud, uso de números, letras, mayúsculas, minúsculas y caracteres especiales, estableciendo su complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso.
- La entidad debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los **privilegios de acceso**, los cuales deben ser administrados y monitoreados por personal autorizado de la entidad.
- La entidad debe cumplir con la arquitectura transversal de validación única del usuario, como única instancia de identificación para la autenticación del usuario, habilitando al usuario para acceder a los sistemas.
- La entidad debe verificar que los administradores de los servicios de red, herramientas y recursos de tecnología **no tengan acceso a sistemas de información en producción**.
- La entidad debe asegurarse que los usuarios o los perfiles de **usuarios que traen por defecto** los sistemas operativos, el firmware y las bases de datos sean eliminados.
- La entidad debe establecer los controles para que los usuarios finales y personal de IT en los servicios de red, recursos tecnológicos y los sistemas de información no tengan instalados en sus equipos de cómputo **utilitarios** que permitan accesos privilegiados a dichos recursos, servicios o sistemas.
- Los administradores de los recursos tecnológicos deben deshabilitar las **funcionalidades o servicios no utilizados** de los sistemas operativos, el

firmware, sistemas, softwares y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.

- La entidad debe revisar periódicamente la actividad de los **usuarios con altos privilegios**, en los registros de auditoría de la plataforma tecnológica y los sistemas de información.
- Se debe monitorear periódicamente los **perfiles de los usuarios** en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos. Se recomienda la creación de módulos para la configuración de los perfiles de usuario en los sistemas de información.
- Las sesiones, passwords, conexiones de acceso, direcciones IP y demás información de acceso utilizada en los códigos fuentes debe ser colocada en **archivos separados del código fuente**, en directorios protegidos contra escritura y accesos no autorizados. Deben tener accesos restringidos de usuarios y permisos.
- Los servidores, dispositivos de comunicación, servicios, equipos y base de datos deben ser configuradas para que solo permitan el acceso desde **los sistemas** específicamente autorizado.
- Los servidores, Base de datos, dispositivos, equipos y servicios deben tener configurados los **usuarios e IP's que podrán acceder** de forma remota.
- Se debe evitar el ingreso a la institución, de equipos, hardware o dispositivos de almacenamiento pertenecientes al funcionario y en caso de permitirse su uso debe ser monitoreado a fin de evitar la extracción no autorizada o perdida de información.
- Las instituciones deberán crear normas y procedimientos de control de acceso a los activos de información

5. LLAVE / TOKEN DE SEGURIDAD

- Los administradores de los tokens deben recibirlos y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de ellos.
- Los usuarios de los tokens serán responsables por los archivos o transacciones que se ejecuten con dicha clave o tokens.
- Los administradores de los tokens deben crear los usuarios y perfiles en cada portal o sitio de uso, según las actividades que realizará cada usuario, quedando registrado en una bitácora.
- Los administradores de tokens deben entregar a los funcionarios designados los usuarios y seriales de los dispositivos que son asignados para su uso, formalizando la entrega por medio de acta y sobre de seguridad para custodia de los mismos, esta actividad quedará registrada en la bitácora.
- El usuario de tokens deben dar de avisos a la entidad en caso de robo o pérdida

de estos con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.

- Los administradores deben realizar cambios de los tokens cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio de titular. Reportando a la entidad y devolviendo los dispositivos asignados. Estas actividades deben quedar registradas en la bitácora.

6. CRIPTOGRAFÍA

- **Todos los canales de accesos a la información**, como red alámbrica o inalámbrica ya sea pública o red interna, equipos de comunicaciones, aplicaciones, interfaz o conexiones con otros sistemas o servicios, interfaz o conexión con bases de datos o archivos, canales de accesos a los servidores, equipos tecnológicos u otros equipos, sensores o dispositivos inteligentes (Smart), medios electrónicos, datos de contraseña y elementos que contengan información sensitiva deben ser seguros utilizando **cifrado**, además de los controles de **autenticación e integridad criptográfica**, como las firmas digitales, códigos de autenticación de mensajes o gestión de claves criptográficas.
- La protección que habrá que proporcionar a la información con mecanismos criptográficos será proporcional al daño que se podría causar si fallara dicha protección. Se deberá valorar y verificar la protección por medio del adecuado funcionamiento de los softwares, hardwares y mecanismos criptográficos.
- Los servicios de protección de información clasificada llevarán registro de: Las zonas de acceso restringido donde se ubican las cuentas cifradas y Los usuarios autorizados para acceder a las cuentas de cifradas.

7. SEGURIDAD EN LA GESTIÓN DE OPERACIÓN

- Identificar, controlar, monitorear y mantener el **registro de las configuraciones** precisas de los sistemas, softwares, bases de datos, servicios, conexiones y demás componentes relacionados con el TIC y permitidos en las estaciones de trabajo, celulares, equipos inteligentes y revisarlos periódicamente.
- Salvaguardar los derechos de la propiedad Patrimonial, portabilidad, distribución y recuperación de los datos generados y procesados de acuerdo al ciclo de vida de la información, incluyendo las acciones de cambios, control de versiones y el borrado seguro.
- Monitorear y establecer **controles de verificación de licencias** actualizadas en los equipos, software, bases de datos y sistemas virtualizados.
- **Identificar y establecer los contactos, proveedores** y organismos

reguladores, autoridades gubernamentales, asociaciones y operadores de servicios para la efectiva actuación ante incidentes internos graves de seguridad según la criticidad de la incidencia, a fin de poder identificar el contacto a localizar según la criticidad.

- Las solicitudes de **acceso al centro de cómputo** o áreas de cableado deben ser aprobadas por funcionarios autorizados. Los visitantes siempre deberán estar acompañados de un funcionario de IT de la institución. Se recomienda que la solicitud de acceso sea mediante nota formal enviada 24 horas antes al funcionario responsable. Toda visita o acceso al TI debe registrarse en la bitácora.
- La entidad puede conceder **accesos temporales y controlados** a los proveedores cuando necesiten realizar las actualizaciones sobre el sistema operativo, así como monitorear dichas actualizaciones. Los proveedores deberán especificar la periodicidad de los accesos en caso que sean programados.
- La entidad debe establecer las **restricciones y limitaciones para la instalación de software** en los equipos de cómputo y servidores con otros sistemas instalados.
- **Los cambios** (adiciones, modificaciones, eliminación) en las instalaciones, sistemas operativos, cambios de tipos de servicios, aplicaciones, bases de datos y redes deben ser gestionados, controlados y registrados de preferencia en un sistema para su gestión.
- Se recomienda la creación de un **Comité de Cambios** para llevar a cabo la planificación, implementación y gestión de los cambios.
- Las entidades deberán realizar un análisis de **impacto de cambio** y mantener ambientes de **prueba y pre-producción** iguales al ambiente de producción, para realizar las pruebas y análisis de vulnerabilidad correspondientes en cada área antes de aplicar los cambios en el área de producción.
- Las plataformas, almacenamientos, servidores e infraestructuras deben estar divididas y clasificadas en zonas de seguridad con funciones, servicios, usuarios, administración, tipo de datos y requerimientos de acceso a estos espacios.
- La dirección de IT debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma y en plataformas críticas se aplica mantenimiento predictivo.
- Se deberá contemplar, monitorear y mantener la capacidad de procesamiento y almacenamiento requerida en los recursos tecnológicos y sistemas de información de la entidad, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.
- El retiro, reparación o instalación de algún componente de hardware o software debe ser realizado únicamente por personal de IT o por proveedores supervisados por personal de IT.

- La jurisdicción del dato debe ser tomado en cuenta cuando se trata de datos privados, confidenciales y de acceso restringido, sobre todo en tecnologías como la nube, donde las responsabilidades, control de accesos, mantenimientos, servicios y actualizaciones, deben estar formalmente y claramente definidas.
- Se requieren instalar y mantener herramientas tecnológicas actualizadas para el control y monitoreo de la seguridad, para impedir el **código malicioso**, virus, malware, spyware, entre otros. Los usuarios que hacen uso de equipos de cómputo deben conocer estas herramientas y aplicar las medidas de prevención del código malicioso.
- Evaluar y seleccionar las herramientas de seguridad informática e implantar controles tecnológicos para proteger la información.
- Todos los contratos de servicios con proveedores deben tener especificado los **Niveles de Servicio** aceptables e inaceptables y las responsabilidades de ambas partes en materia de seguridad de la información. En atención a las incidencias, el proveedor debe cumplir por niveles de criticidad de las incidencias a manera que pueda atender los casos de urgencia de manera inmediata.
- La entidad gubernamental debe monitorear y auditar de forma inmediata y eficiente las situaciones, incidentes o problemas de impacto o urgencia, medir el desempeño del servicio y SLA brindado por el proveedor, dar seguimiento a los contratos y revisarlos periódicamente con el fin de cumplir con las prioridades y necesidades de la entidad.
- Establecer un control de administración, monitoreo y supervisión de todos los niveles y capas de la arquitectura, revisando y monitoreando las redes, servidores, máquinas virtualizadas (en caso de contar con dicha tecnología), bases de datos, aplicaciones, servicios, comunicaciones y flujos de red para detectar posibles ataques, fallas de seguridad, eventos, incidentes o problemas. La periodicidad o continuidad de la supervisión y monitoreo dependerá de la importancia del sistema que establezca la institución y de la confidencialidad de la información.
- Efectuar auditorías aleatorias en todos los niveles, bases de datos, aplicaciones, redes y comunicaciones, servidores, al igual análisis forenses en casos que lo requieran,
- Se debe establecer procedimientos para **cambios en la configuración y actualización** de sistemas operativos, base de datos, equipos y dispositivos de comunicación, softwares y sistemas de seguridad, ejerciendo la gestión del cambio.
- La entidad debe mantener las redes de datos seguras, segmentadas por: dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la entidad, realizando las configuraciones de los dispositivos de seguridad y de red de la plataforma tecnológica.
- La entidad debe **establecer responsabilidades y procedimientos** para

controlar la instalación del software operativo o cualquier otra actualización de softwares, hardware, dispositivos, equipos o servicios, manteniendo un registro en **bitácora** del detalle de las instalaciones, actualizaciones y eliminaciones realizadas por equipos o servicios.

- La entidad debe validar los **riesgos que genera la migración** hacia nuevas versiones del sistema operativo.

8. SEGURIDAD EN ADQUISICIONES, DESARROLLO Y MANTENIMIENTO DE SOFTWARES

Para la adquisición y aceptación de estos tipos de softwares:

i. Softwares desarrollado con **derecho patrimonial de la institución**.
ii. Softwares licenciado con **derecho patrimonial del proveedor**.

- **La entidad** debe establecer metodologías que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de utilizar softwares seguros y proporcionar una visión clara de lo que se espera.
- **Los desarrolladores o proveedores** deben documentar **los requerimientos** y definir la **arquitectura** de software más conveniente y actualizada para cada sistema de información que se quiera implementar, de acuerdo con los requerimientos de seguridad y los controles deseados.
- Todos los sistemas, softwares, aplicaciones y herramientas deben tener un conjunto de **manuales**, al menos el manual de usuario, manual técnico y manual de instalación. El manual técnico debe especificar y detallar claramente el diseño de la arquitectura y los elementos de seguridad considerados para la aplicación a nivel de base de datos, aplicaciones, comunicación, servicios, interfaz, código fuente, el uso de certificados, tokens, encriptaciones o claves, sistema operativo y demás niveles la seguridad colocadas en todo el sistema informático y componentes que contenga la aplicación.
- Se debe validar que los desarrolladores o proveedores certifiquen que todo sistema de información o software adquirido o desarrollado de código fuente, utilice **lenguajes de programación reconocidos** en el mercado y que establezcan claramente si es adquirida con **derechos de propiedad patrimonial** (de la institución) **ó** si es adquirida como **licencias de uso** (con derecho patrimonial del proveedor).
- Se debe deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Se debe verificar que los desarrolladores o proveedores utilicen las **normas (OWASP, W3C)** por la entidad para el desarrollo de aplicativos.
- Se debe validar que los desarrolladores o proveedores certifiquen la transmisión de información relacionada con pagos y transacciones en línea a los encargados por medio de canales seguros.

- La entidad debe crear ambientes separados de desarrollo, pruebas, pre-producción y producción, cada ambiente debe estar separado a nivel físico y lógico. Contando cada uno con su plataforma, servidores, webservice, aplicaciones, usuarios, llaves, claves de acceso y dispositivos independientes de los demás ambientes. Los ambientes de pre-producción y desarrollo no deben afectar producción y deben ser ambientes completamente separados.
- La entidad debe asegurar, mediante los controles necesarios que los usuarios utilicen diferentes perfiles, claves, roles y diferentes token y llaves, para los ambientes de desarrollo, pruebas, pre-producción y producción, asegurándose que existe un acceso diferente (password, usuarios, IP y token) para cada ambiente y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
- La entidad debe establecer el procedimiento y los controles de acceso a los ambientes de desarrollo, prueba y producción de los sistemas de información, manteniendo una bitácora de los perfiles y roles para cada ambiente.
- La entidad debe asegurarse que los **desarrolladores o proveedores internos o externos**, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- La entidad debe asegurarse de la inexistencia de compiladores, editores o fuentes en los ambientes de pre-producción y producción.
- La entidad debe proporcionar **repositorio** de archivo o código fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso da dichos archivos.
- Se debe contar con un **sistema de control de versiones** para administrar los cambios de los sistemas o softwares.
- Las entidades deben **aprobar las migraciones** entre los ambientes de desarrollo, pruebas, pre-producción y producción de los softwares nuevos y/o de cambios o nuevas funcionalidades, manteniendo la **bitácora de las migraciones** realizadas y documentando la forma en que se realizaron.
- La entidad debe implantar controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas, pre-producción y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios. Se recomienda que sea aprobada por un **Comité de Migración**.
- La entidad debe certificar que la información a ser entregada a los desarrolladores o proveedores para sus **pruebas será enmascarada** y no revelará información confidencial de los ambientes de producción.
- La entidad debe eliminar la información de los ambientes de pruebas, una vez hayan concluido.
- La entidad debe generar pruebas a los softwares desarrollados o adquiridos verificando que cumplan con la seguridad necesaria.
- Los desarrolladores o proveedores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

- Los desarrolladores o proveedores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implemente controles de dichas contraseñas.
- Los desarrolladores o proveedores deben establecer los **controles de autenticación** de tal manera que cuando fallen, lo hagan de una forma segura, indicando en la bitácora de la entidad cual fue la falla especifica durante el proceso de autenticación y al usuario final se debe evitar indicar la falla especifica, en su lugar, generando mensajes generales de falla.
- Los desarrolladores o proveedores deben asegurar que no se **despliegan** en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.
- Los desarrolladores o proveedores deben implementar que se **inhabiliten** las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- Los desarrolladores o proveedores deben indicar que se utiliza la **reasignación** de contraseñas, únicamente se envíe un enlace a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben forzar el cambio de las contraseñas temporales después de su utilización.
- Los desarrolladores o proveedores deben implementar que el **último acceso** (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información, se sugiere que el último acceso del usuario se muestre en un cintillo en el sistema de información en la pantalla inicia después de haber iniciado sesión.
- Los desarrolladores o proveedores deben asegurar la **re-autenticación** de los usuarios o efectuar un proceso adicional de confirmar la identidad del usuario en el registro antes de acceder a ciertos recursos o sistemas o la realización de operaciones críticas en los aplicativos.
- Los desarrolladores o proveedores deben, a nivel de los aplicativos, **restringir acceso** a webservices o servicios web, IIS, apache, archivos, directorios u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración solamente a usuarios autorizados.
- Los desarrolladores o proveedores deben implementar en los sistemas la función de configuración para que periódicamente se re-valide la **autorización** de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados. El tiempo o periodo debe ser configurado por el administrador de la aplicación.
- Los desarrolladores o proveedores deben establecer el **tiempo de duración de las sesiones activas** de las aplicaciones y de las cookies, terminándolas una vez se cumpla este tiempo.
- Los desarrolladores o proveedores deben asegurar que no se permiten **conexiones recurrentes** a los sistemas de información construidos con el

mismo usuario.

- Los desarrolladores o proveedores deben construir los aplicativos de tal manera que efectúen **validaciones** de los datos de entrada (campos de formularios, campos ocultos, cabeceras, cookies, queries a la base de datos, url, otros). Se recomienda realizar validaciones en positivo (listas blancas), especificando lo único que se permite en la entrada.
- Los desarrolladores o proveedores deben asegurarse de la generación de los **datos de salida** de manera confiable, utilizando rutinas de **validación centralizadas y estandarizadas**, evitando enviar los datos en url y enviarlos de forma oculta o segunda plano y solicitar confirmación por parte del solicitante antes de ejecutar algún proceso.
- Los desarrolladores o proveedores deben asegurarse que los sistemas de información **validen la información** introducida por usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos de los datos, longitud de los datos, listas de caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros; también debe mostrar mensajes de ayuda donde indique el ingreso de un dato incorrecto o que no es compatible con el formato del campo.
- Los desarrolladores o proveedores deben suministrar opciones de **desconexión** o **cierre de sesión** de los aplicativos (logout) que permiten terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas **protegidas por autenticación**.
- Los desarrolladores o proveedores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como **tokens** o el ingreso de parámetros adicionales de verificación.
- Los desarrolladores deben asegurar que los aplicativos proporcionen la **mínima información de la sesión** establecida, almacenada en cookies y complementos, entre otros.
- Los desarrolladores o proveedores deben garantizar que no se divulgue información sensible como **respuestas de error**, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Los desarrolladores o proveedores deben **prevenir** mostrar la **estructura de directorios** de los sistemas de información construidos.
- Los desarrolladores o proveedores deben mostrar solo la información necesaria. Remover información en los **encabezados** de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores o proveedores deben **evitar incluir** las **cadenas de conexión a las bases de datos en el código de los aplicativos**. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda **que estén cifrados**. No usar usuarios admin en la conexión, el usuario de la conexión de la BD debe tener permiso restringido.

- Los desarrolladores o proveedores deben asegurarse del **cierre de la conexión** a las bases de datos desde los aplicativos tan pronto como éstas no sean requeridas.
- Los desarrolladores o proveedores deben crear **controles** necesarios para la **transferencia de archivos**, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos sólo tengan privilegios de lectura.
- Los desarrolladores o proveedores deben **proteger el código fuente** de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los administradores o proveedores de la aplicación deben verificar que no se permita que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.
- Los desarrolladores o proveedores deben garantizar que las aplicaciones generen **registros (logs)** de auditoría de las **actividades realizadas por los usuarios finales** y administradores en los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.
- Los desarrolladores o proveedores deben garantizar que las aplicaciones generen registros en los logs de **auditoría**, eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas de controles de acceso, intentos de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la entidad. Se debe registrar como mínimo el usuario, la IP, la fecha, hora, y el código de error.
- La entidad designará responsables y establecerá procedimientos para controlar la **instalación de sistemas operativo**, se cerciorará de contar con el soporte de proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado, debiendo realizar pruebas antes de la actualización del ambiente de producción. La aprobación de las instalaciones y actualizaciones deberá quedar registrado.

9. SEGURIDAD EN LOS DISPOSITIVOS MÓVILES GUBERNAMENTALES

- La entidad debe **verificar y validar la protección** de los dispositivos móviles gubernamentales.
- Se debe hacer **nota formal para la entrega de estos equipos** con todas estas instrucciones de la entidad, para garantizar la responsabilidad del usuario con el equipo.

- La entidad debe **establecer las configuraciones y softwares aceptables** en los dispositivos móviles.
- Se debe establecer un **método de bloqueo** como: patrones, contraseñas, biométricos, reconocimiento de voz, entre otros para los dispositivos móviles gubernamentales.
- Se debe activar la opción de **cifrado de memoria** de almacenamiento de los dispositivos móviles gubernamentales para impedir la copia o extracción de datos si el método de desbloqueo (contraseña, biométrico, otros) esta errado o no coincide con el registrado.
- La entidad debe configurar la opción de **borrado remoto** de la información de los dispositivos móviles gubernamentales para evitar la divulgación no autorizada de información confidencial en caso de pérdida o hurto.
- Se debe configurar la opción de **copias de seguridad** de la información de los dispositivos móviles gubernamentales.
- Se debe realizar la instalación de un **software de antivirus** en los dispositivos móviles gubernamentales.
- Se debe activar los **códigos de seguridad de las tarjetas SIM** para los dispositivos móviles gubernamentales y deben ser almacenados por parte de la entidad en un lugar seguro.
- Los usuarios deben evitar utilizar los dispositivos móviles institucionales en lugares que no ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios no deben modificar las **configuraciones de seguridad** de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los usuarios deben **evitar la instalación de programas** desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales provisto con ellos al momento de su entrega.
- Los usuarios deben, cada vez que el sistema de sus dispositivos móviles institucional notifique que hay **actualizaciones disponibles**, aceptar y aplicar la nueva versión.
- Los usuarios deben evitar conectarse a **redes inalámbricas** de uso público así como se recomienda que sean desactivadas en los dispositivos móviles institucionales asignados. Podrán conectarse a las redes inalámbricas públicas cuando estén en misión oficial fuera de la institución
- Los usuarios no deben almacenar videos, fotografías e información personal en los dispositivos móviles institucionales.

10. SEGURIDAD EN LAS COMUNICACIONES

- Las comunicaciones y servicios de red (telefonía, video, internet y otros) deben ser asegurados con protocolos, canales, herramientas, softwares, tecnologías de seguridad y mecanismos de protección contra ataques internos o externos a la institución o para obtener información confidencial o privilegiada de la institución, a fin de establecer y mantener las comunicaciones e información segura.
- La entidad debe poseer las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.
- Mantener separadas las redes para el acceso y servicio de la ciudadanía y visitantes, de la red de la entidad.
- Es preferiblemente mantener las **bases de datos sin internet.**
- **Instalar antivirus** que protejan los equipos frente a la posibilidad de sustraer información del sistema por medio de algún software malicioso.

Correo Electrónico

- La entidad debe **instalar, implementar y utilizar un sistema de protección de correo electrónico, actualizando constantemente** antivirus, antimalware, antispam, antispyware, entre otros sistemas de protección, que reduzcan el riesgo de afectación de la información que se encuentra contenida y transmitida por el servicio de correo electrónico.
- Todas las entidades deben **ejecutar** el software de antivirus, antispyware, antispam, antimalware **sobre los archivos y/o documentos** que son abiertos o ejecutados por primera vez y monitoreándolos constantemente, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- La entidad debe generar y divulgar las **políticas para el uso de correo** electrónico.
- La entidad debe proveer un **ambiente seguro y controlado** para el funcionamiento de la plataforma de correo electrónico.
- La entidad debe establecer **procedimientos** e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- Se debe establecer que las **cuentas de correo** electrónico son asignadas de manera individual, por lo que ningún funcionario de la entidad debe utilizar una cuenta de correo electrónico que no sea suya.
- Se debe establecer que los mensajes y la información contenida en los correos electrónicos sea sólo de uso para sus **funciones dentro de la entidad**.
- Se debe prohibir que los usuarios de correo electrónico envíen **correos masivos** de cualquier tipo que degraden la condición humana o información que no esté relacionada a la institución.
- El departamento de tecnología debe **administrar y controlar** los usuarios que tienen perfiles con autorización de enviar **correos masivos**.

- Se debe establecer que todos los mensajes enviados respeten los estándares, normas, formatos e imagen de la entidad.
- Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir **información sensible** de la entidad. La entidad debe establecer políticas para enviar la información sensible.
- Los usuarios deben ser capacitados para **no abrir correos electrónicos** o sus adjuntos que sean detectados por el sistema de protección o sean sospechosos de tener algún virus, malware u otro.
- Los usuarios deben asegurarse que los **archivos adjuntos** de los correos electrónicos que descarguen de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- **Los usuarios al detectar posibles infecciones de software maliciosos** deben **notificar** a la dirección de tecnología de la entidad para que tome las medidas de control correspondientes.
- La institución debe asegurar la protección de la información en el momento de ser transferida o intercambiada con otras entidades y deberá establecer los **procedimientos y controles** necesarios para el intercambio de información; así mismo, se establecerán acuerdos de confidencialidad y/o de intercambio de información con las terceras partes con quienes se realice dicho intercambio incluyendo los compromisos adquiridos y las penalidades civiles. Las instituciones deben utilizar tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.
- Implementar filtros de protección **contra ataques de Denegación de Servicio Distribuido (DDoS).**
- Las redes de datos deben ser **segmentadas por dominios o grupos** tales como grupos de servicio, grupos por ubicación geo política, grupos de usuarios, configurando los dispositivos de acuerdo al estándar de configuración adoptado por la institución.
- Implementar el uso de **Cortafuegos (Firewall) para hardware y software**, evitando el acceso no autorizado a los dispositivos.
- Se debe utilizar un **sistema de prevención de Intrusos (IPS) y sistemas de detección de intrusos (IDS)** de acuerdo al nivel de riesgo de la información.
- Implementar el uso de **corta fuegos de aplicación (WAF),** cuando el nivel de riesgo de la información así lo requiera.

11. SEGURIDAD DE LOS RECURSOS HUMANOS

- El personal debe **ser capacitado** sobre el tema de la seguridad de la información y el personal externo que presta algún tipo de servicio a la entidad, debe recibir el entrenamiento apropiado.
- El personal debe ser capacitado para conocer las aplicaciones que posee la entidad, monitorearlas y gestionarlas de forma eficiente.
- Concientizar a los **usuarios y proveedores** acerca de sus obligaciones en la seguridad de la información, estableciendo **procedimientos disciplinarios** formales y **firmando documentos** donde se comprometen con dichas obligaciones.
- Todos los **funcionarios y proveedores** que realice o presten algún servicio relacionado con informática, están obligados a **reportar de forma inmediata** los incidentes, problemas, alertas o eventos, violaciones, sospechas, deficiencias, vulnerabilidades o fallas de seguridad que identifiquen.
- Definir e implementar los **roles de responsabilidad** de las entidades y usuarios para el acceso y manejo de la información.
- Los departamentos de las entidades gubernamentales que **procesan datos** personales de funcionarios, proveedores o personas externas deben asegurar que solo aquellos usuarios pertinentes puedan tener acceso a dichos datos.
- Los departamentos de las entidades gubernamentales que procesan datos personales de funcionarios, proveedores y personas externas deben establecer condiciones de seguridad a las entidades vinculadas para el tratamiento de dichos datos.
- Los departamentos de las entidades gubernamentales que procesan datos personales de funcionarios, proveedores y personas externas deben acoger las políticas y procedimientos establecidos para el intercambio y manipulación de los datos, formalizándolo mediante documento firmado por los involucrados.

12. ANÁLISIS Y GESTIÓN DE RIESGO

- Se deberá analizar y evaluar los riesgos de seguridad para determinar los niveles de riesgos permitidos y crear las estrategias de protección a seguir. Estableciendo actores y sus responsabilidades para dar una rápida respuesta y atención al incidente.
- Las entidades deben validar que el procesamiento de datos que realiza se ejecuten sin errores, al igual que debe contar con las métricas necesarias para evaluar el servicio, la disponibilidad, cumplimiento o mejoramiento constante a realizar.
- Mantener una gestión de riesgo continua para minimizar las posibles amenazas futuras.
- La entidad revisará periódicamente la aparición de vulnerabilidades técnicas y de ingeniería social (manipular a los usuarios para obtener información

confidencial), en los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.

- La entidad debe adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético periódicamente establecida, por un ente independiente al área a la que se realizará las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.
- En caso de pérdida o robo de un equipo de cómputo se debe informar de manera inmediata al líder del proceso para que se inicie el trámite interno y se debe reportar el caso frente a la autoridad competente. Si el equipo contiene información confidencial la entidad debe contemplar el uso de herramientas que permitan la información remota.

13. GESTIÓN Y PLAN DE CONTINUIDAD

- La Entidad certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades.
- Las áreas propietarias de la información, con el apoyo de la dirección de tecnología, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.
- La entidad velará porque los medios de almacenamiento con la copia de respaldo de la información crítica sean almacenados en una o varias ubicaciones físicas diferentes a las instalaciones donde se encuentra, pero manteniéndola siempre **dentro del territorio nacional**. Se recomienda que una ubicación sea a varios kilómetros (relativamente cercana y las demás geográficamente distintas en caso de tormentas, maremotos y demás siniestros.
- El sitio externo donde se resguarden las copias de respaldo deben contar con los controles de seguridad física y medioambientales apropiados.
- El personal de IT debe crear, implementar y actualizar los procedimientos y la asignación de responsables que mantengan la disponibilidad e integridad de la información, para las copias de respaldo, su almacenamiento, generación, tratamiento y restauración de la información.
- Se debe realizar una identificación de la ubicación física de los medios de almacenamiento su contenido, fecha de respaldo, con el objetivo de permitir un rápido acceso.
- El personal de IT debe definir las condiciones de transporte, transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente del área de la institución.

- Es responsabilidad de los usuarios identificar la información crítica que debe ser respaldada y almacenada de acuerdo con su nivel de clasificación.
- La entidad deberá definir el **plan de generación, rotación, y retención** de las copias de respaldo de la información, estableciendo la periodicidad de copias de respaldo para la información crítica y el resto de la información, incluyendo copias de respaldo de las configuraciones de hardware, software, equipos de redes y otros.
- Se deberán mantener información **respaldada al menos** dos copias de la información del día: lo más actualizada posible, manteniendo copias de respaldo de la información de los días anteriores al actual, información de la semana anterior, información del mes anteriores.
- Se deberán contar con **planes de continuidad y contingencia del negocio, asignando los funcionarios responsables para ejecutarlo.**
- La entidad deberá contar con **planes de contingencia para la recuperación ante desastres** clasificando cuales serán emergencias o desastres.
- Se deberá contar con **procedimientos escritos de contingencias.**
- Se deberán realizar copias **actualizadas** de seguridad de la información, deberá incluir copia de respaldo de bases de datos, hardwares, sistemas operativos y configuraciones, softwares, dispositivos de comunicaciones, redes y herramientas, con la asignación de funcionarios responsables de realizarla y los recursos necesarios.
- Se realizará las **pruebas de restauración** de las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario por medio del personal de IT. Se recomienda se realicen estas pruebas de restauración de backups periódicamente, como mínimo una vez al año.
- La entidad deberá **crear la documentación de los procedimientos de continuidad**, manteniendo disponible la información escrita vital (reportes, formularios, documentos) para que los servicios críticos continúen.
- Se debe asegurar la realización de **pruebas periódicas del plan de contingencia (recuperación) y del plan de continuidad**, verificando la seguridad de la información durante su realización y la documentación, aplicando distintos tipos de siniestros (fuego total, inundaciones, temblor, perdida permanente de electricidad, entre otros).
- La entidad debe reconocer las situaciones que deberán ser **identificadas como emergencia o desastre** para la entidad y determinar cómo se debe actuar sobre ellas, realizando la protección del personal y la protección del negocio asegurándose que los procesos de negocio críticos estarán disponibles para los usuarios en el **Plan de continuidad**.
- Establecer procedimiento para mantener **alta disponibilidad** en los datos y sistemas que se requieran, generando **redundancia** de bases de datos, webservice (servicios web), hardwares, software, dispositivos de comunicaciones, redes y conexiones, aplicaciones, sistemas, servicios, los cuales deberán ser de acceso y permisos restringidos y la redundancia debe

estar en un lugar geográficamente distinto. Realizando la administración de las soluciones de redundancia y pruebas periódicas, como mínimo anuales.

- Se deberá mantener acuerdos de nivel de servicio que tomen en cuenta la continuidad del negocio mediante contratos escritos donde se estipule el alcance.

14. INCIDENTES DE SEGURIDAD

- La dirección de tecnologia debe definir la realización de monitoreo sobre los registros de auditoria de los aplicativos donde se opera los procesos de la entidad. Se debe realizar la revisión de logs mensuales para analizar los resultados del monitoreo efectuado.
- La entidad debe mantener un registro de **lecciones aprendidas** de incidentes para mejorar los tiempos de respuesta frente a situaciones futuras, se recomienda que este registro sea en un sistema automatizado.
- Los responsables de los archivos de información deberán informar al área de IT de su institución los incidentes de seguridad tan pronto lo detecten u observen algún riesgo.
- La dirección o área de IT debe crear procedimientos y nombrar responsables para actuar frente a incidentes, estableciéndolos para cada tipo de incidente posible.
- La dirección o área de IT, al igual que los proveedores de algún servicio deberán notificar al comité de seguridad o encargado de la seguridad de la información, los casos que se consideren pertinentes.
- El área de IT deberá designar al personal responsable calificado para investigar los incidentes de seguridad, identificando las causas y tomar las medidas necesarias para solucionarlos.
- Los incidentes, eventos y problemas serán registrados, al igual que la respectiva solución, para contar con una **base de conocimiento de errores conocidos.**
- Los responsables de los activos de información deben informar a la entidad los incidentes de seguridad que identifiquen o que reconozcan una alta probabilidad que ocurra. Se debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares.
- Se debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados.

15. INTERCAMBIO DE INFORMACIÓN (INTEROPERABILIDAD)

- Se deben establecer los procedimientos y normas para la interoperabilidad de forma fluida y eficaz.

- La dirección o área de IT deberá realizar los procesos para el intercambio de la información con otras entidades; incluyendo los compromisos, penalidades y acuerdos de confidencialidad si se requiere. Acuerdos más formales deberán ser firmados por el proveedor y el proveedor tiene la obligación de que los subcontratistas establezcan en su contrato que cumplan con dicha responsabilidad de confidencialidad.
- Los responsables de los activos de la información deben asegurarse que la interoperabilidad o intercambio de la información se realice solo entre usuarios o servidores autorizados.
- Los intercambios con información sensitiva o confidencial deben contener datos encriptados o cifrados.
- Se deberán realizar la interoperabilidad entre instituciones tomando en cuenta el diseño de la **arquitectura tecnológica**, se recomienda que la **base de datos** se encuentre en un servidor separado y sin acceso a internet, el **servidor de webservice** en otro servidor separado y desde ese punto se accede con el usuario y permisos respectivos a la base de datos. El **servidor de aplicación** se deberá colocar en otro servidor separado y contendrá el portal del sistema que será accedido por los usuarios.

Base de Datos

- Las Bases de Datos deben tener **definidos los usuarios** que las pueden acceder, con los privilegios, permisos y roles respectivos bien definidos, con mecanismos que limiten el acceso a vistas, relaciones, tablas, datos, entre otros.
- Se deberán **crear distintos usuarios de una base de datos** para que sean utilizados en la **conexión de la aplicación a la base de datos**. Debe existir un usuario creado en la base de datos para que cada aspecto de la aplicación (consulta, adición, eliminación, otros) se conecte a la base de dato con los permisos muy limitados a los objetos de la base de datos y solo para cumplir ese aspecto especifico para el que se conectara la aplicación con ese usuario a la base de datos (ejemplo: aplicación_para_consultas usará el usuario_solo_consulta). Esto evita que se tenga acceso a todos los permisos la base de datos utilizando las credenciales de conexión de la aplicación.
- La Base de datos podrá contener **encriptada o cifrada los datos** que considere la institución de acuerdo a su criticidad o sensitividad.
- Las Bases de datos deben mantenerse en **sitios protegidas** de robo, incendio, inundaciones y otros.
- Los datos deben poder ser **auditados** y las acciones de los usuarios también deben ser supervisados y auditables.
- Se deben realizar todos los **controles, revisiones y procedimientos** necesarios a fin de mantener la integridad de la información.
- El usuario de la base de datos debe realizar dos procesos, el de **identificación y el de autenticación.**
- Evaluar periódicamente las **vulnerabilidades y configuraciones** de las base de datos, aplicando las recomendaciones específicas para corregir las

vulnerabilidades, a este proceso se le conoce como endurecimiento.

- Evaluación y seguimiento de las recomendaciones específicas para corregir las vulnerabilidades.
- Implementación de **alertas automáticas** frente a cambios en la configuración de la base de datos.
- **Monitorear** en tiempo real las bases de datos frente al uso indebido, intrusos o cambios, patrones inusuales de acceso, pudiendo colocar agentes o herramientas para realizar de forma automática el monitoreo.
- **Monitorear** a los usuarios privilegiados.
- Mantenga actualizadas las **versiones** de su base de datos, aplicando los procesos para el control de cambios.
- Verificar el **ambiente de instalación** de la Base de datos, verificación de la forma en que se instaló la base de datos y su sistema operativo (por ejemplo, la comprobación privilegios de grupos de archivo -lectura, escritura y ejecución- de base de datos y bitácoras de transacciones).
- Asimismo con archivos con parámetros de configuración y programas ejecutables.
- El área de IT deberá **facilitar herramientas o servicios para el intercambio de información** segura que faciliten la encriptación o cifrado de los datos.
- Los responsables de los activos de la información o quien ellos deleguen que el intercambio de información con otras entidades quede registrado detallando el tipo de información, el emisor, la fecha y el receptor como los datos mínimos que se deben registrar.
- El intercambio de información debe ser por **canales cifrados seguros** y autorizados.

BIBLIOGRAFÍA

- IsecT LTD, Hinson Gary. ISO/IEC 27002:2013. *Information technology — Security techniques — Code of practice for information security controls (second edition)*. Recuperado de http://www.isect.com.
- López Agustín, Ruiz Javier. *El portal de ISO 27001*. Recuperado de http://www.iso27000.es/
- International Organization for Standardization, ISO Central Secretariat, ISO. ISO/IEC 27017:2015. (2015). Recuperado de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757
- Symantec Corporation; *Glosario de Términos*. Recuperado de https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad.
- Estudio Neobox. (2011). *Glosario de Seguridad Informática*. Recuperado de http://neobox.com.ar/

- Dirección de Presupuesto. (2004). *Norma Técnica para Órganos de la Administración del Estado sobre la Seguridad y Confidencialidad de los Documentos Electrónicos*. Recuperado de http://www.dipres.gob.cl/594/articles-51683_egov_decreto83.pdf
- Wikimedia Foundation, Inc. Wikipedia, the free encyclopedia. https://es.wikipedia.org/wiki/
- Centro Nacional de Respuesta a Incidentes de Seguridad Informática. (2013). *Glosario de Términos*. Recuperado de https://www.cert.uy/inicio/sobre_seguridad/glosario/
- ICETEX. (2014). *Manual de Políticas de Seguridad de la Información*. Recuperado de https://www.icetex.gov.co/
- Olivardia Virgilio, Centauri Technologies Corporation. (2017). *Análisis del esquema de interoperabilidad gubernamental*.
- International Organization for Standardization. *Normas ISO 27000, 27001, 27002, 27005, 27017, 27018, 27036*. Recuperado de https://www.iso.org/popular-standards.html