República de Panamá

AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL

Resolución No. 99
16 de octubre de 2017

"Por la cual se aprueba el documento titulado: **NORMAS GENERALES PARA LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC) EN EL ESTADO**".

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 (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 7 de la Ley 65 de 2009, establece que es función del Administrador General de la AIG, dirigir y administrar esta Entidad.

Que la Ley 83 de 9 de noviembre de 2012, "Que regula el uso de los medios electrónicos para los trámites gubernamentales y modifica la Ley 65 de 2009, que crea la Autoridad Nacional para la Innovación Gubernamental", establece las reglas y principios básicos de obligatorio cumplimiento para la ejecución de los trámites gubernamentales en línea, aplicables al Gobierno Central, entidades autónomas y semiautónomas, municipales, la Asamblea Nacional, el Órgano Judicial, los intermediarios financieros y las sociedades en las que el Estado sea propietario del 51% o más de sus acciones o patrimonio, en sus relaciones entre sí y entre éstas y los usuarios, a fin de que sean aplicados de forma gradual, conforme lo establezcan cada una de éstas.

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 en ejercicio de sus facultades legales, la AIG ha considerado necesario adoptar el documento titulado "**NORMAS GENERALES PARA LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC) EN EL ESTADO**", que tiene como objetivo principal el desarrollo y la protección de los sistemas tecnológicos, mejorar y normalizar los procesos tecnológicos del Estado, procurando fortalecer la infraestructura tecnológica en las instituciones, incorporando pautas de control que deben ser acatadas en la gestión de las tecnologías y el uso de los recursos, lo que finalmente facilitará las labores de control y fiscalización sobre los mismos, por lo que el suscrito,

RESUELVE:

PRIMERO: Aprobar el documento titulado: **"NORMAS GENERALES PARA LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC) EN EL ESTADO"**, tal cual se adjunta a la presente Resolución.

SEGUNDO: La Autoridad Nacional para la Innovación Gubernamental (AIG) por conducto de la Dirección de Gobernanza de Tecnologías de la Información (TI), será la responsable del seguimiento, coordinación y control de las Normas Generales para la Gestión de las Tecnologías de la Información y Comunicaciones (TIC), en el Estado; para lo cual elaborará informes y publicará el "Ranking de Cumplimiento" por parte de las entidades estatales.

TERCERO: Ordenar la publicación de la presente Resolución en la 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 No. 205 de 9 de marzo de 2010, Decreto Ejecutivo No. 719 de 15 de noviembre de 2013, Decreto Ejecutivo No. 357 de 9 de agosto de 2016.

PUBLÍQUESE Y CÚMPLASE,

IRVIN A. HALMAN
ADMINISTRADOR GENERAL

AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL
DESPACHO SUPERIOR

IAH/GR/JP/TB/jvm

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

Autoridad Nacional para
la Innovación Gubernamental
innovamos para ti

GOBIERNO DE LA REPÚBLICA DE
PANAMÁ

Normas Generales para la Gestión de las Tecnologías de la Información y Comunicación en el Estado

AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL (AIG)

Dirección Nacional de Gobernanza de TI

29 de agosto de 2017

IRVIN A. HALMAN
Administrador General

LUIS FASANO
Subadministrador General

GABRIEL REYES
Director de Gobernanza de Tecnología de Información

JOAQUÍN HUERTAS
Director de Servicios de TI

TERESA BERBEY
Jefa de la Oficina de Asesoría Legal

GISELA GONZÁLEZ
Jefa de la Oficina de Auditoría Interna

SILVIA BATISTA
CSIRT Panamá

JULIO PRESTAN
Dirección de Gobernanza de TI

Fecha	29.08.2017
Versión	Lanzamiento #1, Versión 19
Nivel de difusión	Público
Estatus	Documento Final
Documento aprobado por	Irvin A. Halman

ÍNDICE

1 Introducción

La Autoridad Nacional para la Innovación Gubernamental (AIG) ha establecido la presente Norma General para la Gestión de las Tecnologías de Información y Comunicación (TIC) con el objetivo principal de normalizar los procesos relacionados en el sector público, además de contribuir al fortalecimiento de los sistemas e infraestructura tecnológica en las entidades del Estado, incorporando lineamientos de control, los cuales deben ser acatados en la gestión y en el uso de los recursos de las TIC, así como para facilitar las labores de control y fiscalización.

Cada norma ha sido clasificada y definida mediante una descripción, acompañada de una justificación que explica su objetivo primordial o su marco regulatorio.

Se requiere de las entidades del Estado el cumplimiento de las recomendaciones o sugerencias, con lo cual se asegura el fortalecimiento institucional, la interoperabilidad de datos, los niveles de servicio y seguridad en el sector público.

Acorde a las necesidades y avances en la materia, esta primera versión del documento podrá sufrir cambios o actualizaciones, acorde a los procedimientos que establezca la AIG para tal efecto.

2 Sujetos de la Norma

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 Entidad 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 Unidad de Tecnología de la Información (TI), el cumplimiento de la Norma y su difusión a los miembros de la Entidad que regenten.

3 Marco Legal

Ley N°65 del 30 de octubre de 2009, en su artículo 1 dispone que la AIG es la entidad competente del Estado para planificar, coordinar, emitir directrices, supervisar, colaborar, apoyar y promover el uso óptimo de las tecnologías de información y comunicaciones en el sector gubernamental para la modernización de la gestión pública, así como recomendar la adopción de políticas, planes y acciones estratégicas nacionales relativas a ésta materia.

El marco legal que fundamenta a ésta Norma, lo componen las leyes y decretos ejecutivos emitidos que enumeraremos a continuación:

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

Decreto Ejecutivo N° 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".

Ley 83 de 9 de noviembre de 2012, "Que regula el Uso de Medios Electrónicos para los Trámites Gubernamentales y modifica la Ley 65 de 2009, que Crea la Autoridad Nacional para la Innovación Gubernamental"..

Decreto Ejecutivo Nº 719 de15 de noviembre de 2013, "Que reglamenta la Ley 83 de 9 de noviembre de 2012, que regula el uso de medios electrónicos para los trámites gubernamentales y modifica la Ley 65 de 2009, que crea la Autoridad Nacional para la Innovación Gubernamental".

Decreto Ejecutivo Nº 357 de 9 de agosto de 2016, "Que modifica el Decreto Ejecutivo N° 719 de 15 de noviembre de 2013 y dicta otras disposiciones para la ejecución de acciones de modernización gubernamental y de gobierno digital".

Decreto Ejecutivo N° 584 de 26 de julio de 2011, "Por el cual se crea el Centro de Atención Ciudadana 311 y se deja sin efecto el Decreto Ejecutivo N° 555 de junio de 2010".

Decretos Ejecutivos N° 272 de 14 de abril de 2015, "Que modifica artículos al Decreto Ejecutivo N° 584 de 26 de julio de 2011, por el cual se crea el Centro de Atención Ciudadana 311 y se deja sin efecto el Decreto Ejecutivo N° 555 de junio de 2010".

Resoluciones:

- Resolución 15-2016 Aprueba Esquema de Interoperabilidad CNIG, "Por lo cual se aprueba el esquema de Interoperabilidad Gubernamental como parte del sistema nacional de Interoperabilidad y Seguridad" o vigente.
- Resolución No. 14 del 10 de febrero de 2015 y publicado en Gaceta Oficial No. 27730 -A lunes, 2 de marzo de 2015, "Guía para la Obtención del Concepto Favorable de la Autoridad Nacional para la Innovación Gubernamental (AIG) para la Contratación de Bienes o Servicios de Tecnologías de la Información y Telecomunicaciones" o vigente.
- Resolución No. 293 del 18 de febrero de 2013 y publicado en Gaceta Oficial No. 27246-B del 15 de marzo del 2013, "Estándares para la Creación y Uso de las Redes Sociales en las Entidades del Gobierno de Panamá" o vigente.
- Resolución No. 234 de 2 de Agosto, 2012, publicado en Gaceta Oficial No. 2709, "Por la cual se aprueban los Estándares de Calidad para software en las entidades del Gobierno de Panamá" o vigente.
- Resolución No. 60 de 20 de Abril, 2011, publicado en Gaceta Oficial No. 26772-B, "Por la cual se aprueban las Directrices para los Pagos que sean realizados por Medios Electrónicos a favor de las Entidades Gubernamentales, recogidas en el documento denominado "Estándares de Gobierno para Pagos Electrónicos" o vigente.
- Resolución No. 55 de 01 de Marzo, 2011, publicado en Gaceta Oficial No. 26749-A, "Por la cual se aprueban los Estándares para Páginas Web en las Entidades del Gobierno de Panamá" o vigente.
- Resolución No. 54 de 01 de Marzo, 2011, publicado en Gaceta Oficial No. 26737-C, "Por la cual se aprueban los Estándares de Gobierno para Cableado Estructurado" o vigente
- Resolución No. 42 de 07 de Enero, 2011, publicado en Gaceta Oficial No. 26697, "Por la cual se aprueban los Estándares para la Estructura, Dominio y Uso del correo electrónico del Gobierno" o vigente.
- Resolución No. 7 de 03 de Junio, 2010, publicado en Gaceta Oficial No. 26547-A, "Por medio de la cual se adopta la Hora Nacional de Panamá, según definición del CENAMEP AIP, como la Hora Oficial para todas las Entidades del Estado" o vigente.
- Resolución N° 12 de 9 de marzo, 2017, "Guía para la Implantación y Gestión de Casos Recibidos por medio del Centro de Atención Ciudadana (CAC) 311en las Entidades del Estado", o vigente.

4 Cumplimiento de los preceptos de la Ley 83 de 9 de noviembre de 2012, su reglamentación y otras disposiciones

4.1 Trámites Registrados en el Portal Oficial "Panamá Tramita"

Norma: La Entidad debe comunicar y mantener actualizado el Portal Oficial **www.panamatramita.gob.pa,** con la información de TODOS los trámites disponibles Y LOS REQUISITOS NECESARIOS para su ejecución por parte de los ciudadanos, contribuyentes y público en general.

Justificación: Cumplimiento del Reglamento y apoyo a las iniciativas estratégicas del Estado. Art. 11, del Decreto Ejecutivo N° 719 de 2013, ampliado por el Decreto Ejecutivo N° 357 de 2016.

4.2 Formularios para la gestión de los Trámites

Norma: Cuando el trámite incluye el uso de formularios como parte de la gestión, la Entidad debe proveer los formularios, en formato abierto en el Portal Oficial "Panamá Tramita" con la opción de descarga del documento. Este Portal es administrado por la Oficina de Gobierno Electrónico de la AIG.

Justificación: Cumplimiento del Reglamento y apoyo a las iniciativas estratégicas del Estado. Art. 11, del Decreto Ejecutivo 719 de 2013, ampliado por el Decreto Ejecutivo N° 357 de 2016.

4.3 Trámites en Línea

Norma: La Entidad debe brindar, en la medida de sus posibilidades, la opción de gestión de sus trámites "en línea". Progresivamente puede aplicar estas opciones:

La Entidad permite iniciar el trámite en línea, pero el ciudadano deberá apersonarse a la misma para completar la gestión del trámite.

La Entidad permite realizar completamente el trámite en línea, así como publicar el estado del trámite en los casos que haya pasos intermedios. Cuando la entidad disponga de un trámite a éste nivel, deberá publicitar la información en los medios de comunicación y en el Portal Oficial "Panamá Tramita".

Justificación: Cumplimiento del Reglamento y apoyo a las iniciativas estratégicas del Estado. Capítulo 1, del Decreto Ejecutivo 719 de 2013, ampliado por el Decreto Ejecutivo N° 357 de 2016.

4.4 Plan de Simplificación de Trámites

Norma: La Entidad elaborará anualmente un Plan de Simplificación (progresiva) de sus procesos administrativos y trámites que guarden relación con los ciudadanos. El "Plan" debe ser aprobado por la AIG.

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 18, Ley 83 de 2012.

4.5 **Aceptación de documentos firmados electrónicamente por los usuarios**

Norma: Los Sistemas para la Gestión de Trámites o Servicios en línea admitirán, en los casos que aplique, los documentos firmados electrónicamente por el ciudadano o contribuyente, y estos tendrán la misma validez que los documentos firmados de manera autógrafa u hológrafa.

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 4. numeral 10, Ley 83 de 2012.

4.6 **Excepción de los usuarios de aportar datos y/o documentos, cuando ya posean información en las bases de datos de entidades públicas**

Norma: Cuando la información del usuario se encuentre en una Base de Datos del Estado, éste estará exento de aportar sus datos y/o documentos para el trámite que realice. La Unidad de TI de la Entidad, deberá implementar procedimientos y/o servicios, que permitan obtener la información de la Base de Datos correspondiente. Esta excepción se hará constar en el correspondiente requisito del trámite en el portal oficial "Panamá Tramita".

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 4 numeral 3, Ley 83 de 2012.

4.7 **Habilitación de diferentes canales o medios para la prestación de trámites**

Norma: La Unidad de TI de la Entidad, en la medida de sus posibilidades, debe habilitar diferentes canales o medios para la gestión de los trámites gubernamentales en línea, sean estos por sitio web, aplicativos móviles, correo electrónico, entre otros medios seguros que estén disponibles para la Entidad.

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 4 numeral 14, Ley 83 de 2012.

4.8 **Uso de la Pasarela y Portal Nacional de Pagos**

Norma: La Unidad de TI de la Entidad, en la medida de sus posibilidades, debe establecer los mecanismos de pago en línea, que permitan a la Entidad suministrar al usuario en tiempo real la información requerida para mantener actualizada la Pasarela y el Portal Nacional de Pagos.

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 20, Ley 83 de 2012.

4.9 **Realizar pagos por transferencia automática de fondos**

Norma: La Unidad de TI de la Entidad, en la medida de sus posibilidades, debe incorporar los componentes necesarios para cumplir con la Ley, en relación a que la entidad efectué el pago de sus obligaciones utilizando la Transferencia Automática de Fondos.

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 21, Ley 83 de 2012.

4.10 **Impulsar el uso del Centro de Atención Ciudadana 311 para asistencia en el uso de los Trámites en línea**

Norma: La Entidad debe promover el uso del Centro de Atención Ciudadana 311, para realizar consultas sobre los trámites en línea.

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 4 numeral 16, Ley 83 de 2012.

4.11 Acceso sencillo y eficaz de la información pública

Norma: Las Entidad debe promover herramientas y buscadores que faciliten a los usuarios el acceso sencillo y eficaz a la información pública por medios electrónicos y debe garantizar la protección de la información confidencial o de acceso restringido. Utilizar esquemas de doble autenticación para evitar la extracción de información de manera masiva.

Por tal razón, recomendamos la revisión de los índices y la arquitectura de los sitios web y aplicaciones móviles para facilitar el acceso del usuario a la información, así como planificar e implementar el suministro de información en formato reutilizable de Datos Abiertos para el acceso, uso y análisis de la información pública.

El Portal Oficial **www.datosabiertos.gob.pa** de Datos Abiertos, administrado por la Oficina de Datos Abiertos de la AIG, está disponible para la publicación de catálogos de datos abiertos de la Entidad que son de interés público.

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 4 numeral 12, Ley 83 de 2012. Decretos Ejecutivos: "Por el cual se crea el Centro de Atención Ciudadana 311 y se deja sin efecto el Decreto Ejecutivo N° 555 de junio de 2010". "Que modifica artículos al Decreto Ejecutivo N° 584 de 26 de julio de 2011, por el cual se crea el Centro de Atención Ciudadana 311 y se deja sin efecto el Decreto Ejecutivo N° 555 de junio de 2010" y "Que modifica el Decreto Ejecutivo N° 719 de 15 de noviembre de 2013 y dicta otras disposiciones para la ejecución de acciones de modernización gubernamental y de gobierno digital".

4.12 Publicaciones electrónicas

Norma: La Unidad de TI de la Entidad, debe habilitar en el sitio web institucional, una sección para la publicación de anuncios, boletines, informes, memorias, edictos, licitaciones, otros, que por disposiciones legales o reglamentarias indican que deben ser publicadas en el tablero de anuncios.

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 6, Ley 83 de 2012.

4.13 Idiomas

Norma: La Unidad de TI de la Entidad, en la medida de sus posibilidades, debe ofrecer versiones en otros idiomas de sus páginas Web, de acuerdo a la operación de la Entidad.

Justificación: Al ofrecer un servicio a los visitantes o residentes extranjeros, la Entidad, de acuerdo a la naturaleza de sus servicios o trámites, permitirá que éstos sean capaces de hacer sus trámites sin necesidad de realizar traducciones.

4.14 Facilitad para los usuarios con discapacidad

Norma: Las Entidad deberá facilitar a los usuarios con discapacidad o con condiciones especiales el acceso a la información que les permita efectuar los trámites en línea, para lo cual se recomienda la utilización de "plug-ins" disponibles para discapacidad visual, auditiva o motora.

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 4 numeral 13, Ley 83 de 2012.

4.15 **Facilitar acceso a información de la Entidad, por parte de otras entidades públicas**

Norma: La Unidad de TI de la Entidad, en la medida de sus posibilidades debe habilitar convenios, protocolos y mecanismos que permitan intercambiar datos dentro de los procesos de trámites, manteniendo niveles aceptables de seguridad en la interoperabilidad.

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 4 numeral 17, Ley 83 de 2012.

4.16 **Cumplimiento de normas, estándares y condiciones en los sistemas tecnológicos**

Norma: La Unidad de TI de la Entidad, debe cumplir con los estándares establecidos, para lo cual la AIG realizará inspecciones, verificando el cumplimiento de las Normas, Estándares y condiciones para el buen uso de los sistemas y equipos.

Justificación: Cumplimiento del Decreto Reglamentario de la Ley 65 y apoyo a las iniciativas estratégicas del Estado. Art. 7 Decreto Ejecutivo N° 205 de 9 de marzo de 2010.

4.17 **Plan de Sistemas**

Norma: La Unidad de TI de la Entidad, debe elaborar su Plan de Sistemas con el objeto de facilitar la correcta apreciación del estado de los sistemas informáticos, los requerimientos, y así poder identificar un estado futuro de dichos sistemas alineados con los objetivos de la entidad.

El Plan de Sistemas de la Entidad debe contener lo siguiente:

- Diagnóstico de la situación informática actual con la finalidad de conocer las capacidades actuales;
- Elaboración de objetivos y estrategias del sistema de información que sirva de base para apoyar la misión y los objetivos institucionales;
- Desarrollo del modelamiento de datos para determinar qué información institucional es necesaria;
- Generación, ordenamiento y priorización (por nivel de importancia e inversión) sistemática de los proyectos informáticos;
- Programación de los tiempos requeridos para la puesta en marcha de los proyectos designados, estimando el periodo de vida de cada proyecto.

Justificación: Cumplimiento del Decreto Reglamentario de la Ley 65 y apoyo a las iniciativas estratégicas del Estado. Art. 43, del Decreto Ejecutivo N° 719 de 2013, modificado por el Decreto Ejecutivo N° 357 de 2016, y Decreto Ejecutivo N° 214 de 8 de octubre de 1999 Normas de Control Interno emitida por la Contraloría General de la República.

4.18 **Agenda Digital Institucional**

Norma: La Unidad de TI de la Entidad deberá elaborar y presentar a la AIG en el último trimestre de cada año, una Agenda Digital Institucional, conteniendo las iniciativas de modernización tecnológica, siguiendo los lineamientos que emita la AIG, y que consisten en incluir las iniciativas de modernización tecnológica programadas a corto (1 año), mediano (3 años) y largo plazo (5 años).

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 19, Ley 83 de 2012, Art. 27 del Decreto Ejecutivo 719 de 15 de noviembre de 2017 modificado por el Artículo 6 del Decreto Ejecutivo 357 de 9 de agosto de 2016.

4.19 **Plan Operativo Anual**

Norma: La Unidad de TI de la Entidad deberá elaborar y presentar a la AIG en el último trimestre de cada año, el Plan Operativo anual del año siguiente, que contiene el planeamiento de los proyectos presupuestados y aprobados.

Justificación: Cumplimiento de la Ley y apoyo a las iniciativas estratégicas del Estado. Art. 19, Ley 83 de 2012.

5 Normas de Aplicación General

5.1 Unidad Ejecutora de Gobierno Digital

Norma: Las Entidad deberá establecer una Unidad Ejecutora de Gobierno Digital al más alto nivel, la que tendrá la responsabilidad de liderar y dar seguimiento a las acciones institucionales establecidas en la Agenda Digital Institucional, en los Planes de Simplificación de Trámites y el Operativo Anual. Además deberá adoptar y dar el seguimiento a los lineamientos que defina la AIG a través de su Dirección de Gobernanza de TI.

La Entidad, a través del Despacho Superior, considerará al Jefe de la Unidad de TI, quien es el enlace ante la AIG, como un integrante de la Unidad Ejecutora y un componente clave en la gestión institucional del Gobierno Digital para la atención en sus áreas de competencia y servicio a sus usuarios.

Se recomienda que el Despacho Superior se apoye con un equipo multidisciplinario institucional, que avale la correspondencia de los proyectos de Gobierno Digital con la estrategia institucional, además de establecer las prioridades de los proyectos de TI y apoyar en la asignación de los recursos.

Justificación: Art. 44, Decreto Ejecutivo N° 357 de 2016. Propiciar el uso de las TIC para el desarrollo del Plan Estratégico institucional e impulsar la incorporación del Gobierno Digital al más alto nivel, que permita el uso eficaz de las herramientas disponibles para la gestión y ahorros de la Entidad.

5.2 Gestión de la Calidad en los Servicios

Norma: La Unidad de TI debe entregar sus productos y servicios, en conformidad con los requerimientos solicitados y con un enfoque de eficiencia, efectividad y mejoramiento continuo de sus procesos y servicios a los usuarios. Recomendamos la implementación de Procedimientos de Control de Calidad, tales como:

- Evaluación de la satisfacción del usuario.
- Control del servicio no conforme.
- Control de la documentación del sistema.
- Gestión de acciones correctivas y preventivas.

Justificación: Estimular la gestión de calidad en los productos y servicios de TI (Soporte Técnico, Desarrollo de Software, otros).

5.3 Gestión de la Seguridad de la Información

Norma: La Unidad de TI debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, en especial de los datos de carácter personal, lo que implica protegerla contra: el uso para la cual no fue obtenida, daño, pérdida o modificación no autorizada. Se recomienda que la Entidad cuente con un profesional de Seguridad de la Información.

En los casos en que la Entidad posea una oficina especializada sobre el tema, como sería el contar con un director de seguridad de la información o CISO por sus siglas en inglés ("Chief Information Security Officer"), a esta le corresponderá como unidad responsable el planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar

la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad.

Para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), en inglés: "Information Security Management System" (ISMS), recomendamos se considere utilizar esencialmente las siguientes normas ISO vigentes:

- 27001 - Modelo para gestionar la seguridad de la información en una organización.
- 27002 - Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

Se recomienda implementar la Norma en las áreas de mejor utilidad para la Entidad, ya sea una dirección, departamento, oficina o dependencia. No tiene que implementarse en toda la Entidad.

Justificación: Promover la adopción de un Sistema de Gestión y la adopción de medidas preventivas y reactivas que permitan resguardar y proteger la información, además de preservar la confidencialidad, la disponibilidad e integridad de la misma.

5.4 Compromiso del funcionario con la seguridad de la información

Norma: Todo funcionario de la Entidad, incluyendo terceros que accedan a la misma, debe estar comprometido con el cumplimiento de los procedimientos para la seguridad de la información. El área responsable en la Unidad de TI de la Entidad debe establecer campañas de concientización dentro de la Entidad, salvo que otra de sus dependencias esté a cargo de esta materia.

Justificación: Promover la responsabilidad del funcionario con el cumplimiento de las políticas establecidas en referencia a la seguridad de la información.

5.5 Seguridad Física del Centro de Datos

Norma: Se debe planificar e implementar un sistema de seguridad perimetral que comprende establecer un sistema de control de acceso electrónico, cámaras de vídeo vigilancia en áreas sensitivas y un registro de ingresos y egresos al área de tecnología.

Justificación: Establecer controles, sistemas o elementos a implementar para el monitoreo, prevención y alertas de eventos de seguridad en los centros de datos.

5.6 La Seguridad en las Operaciones y Comunicaciones

Norma: El área responsable en la Unidad de TI deben implementar o adoptar medidas y/o procedimientos (VPN, Certificados Digitales, otros), que apoyen al funcionario para una correcta y segura ejecución de sus actividades en la red, estableciendo canales de comunicación seguros, a los cuales se deben establecer supervisión.

Justificación: Impulsar la implementación de canales seguros, para dotar de seguridad a las comunicaciones, a la información.

5.7 El Control de Acceso a los Sistemas

Norma: El área responsable en la Unidad de TI debe emplear un procedimiento para la asignación de roles y privilegios, que controle y permita trazabilidad sobre el acceso lógico a

la información y facilite el seguimiento de las operaciones realizadas por los usuarios de los sistemas.

Justificación: Promover el uso del control de acceso para la verificación de una Entidad (persona, computador, otros) que solicita acceso a un recurso y comprobar que cuenta con los derechos y tenga habilitado un registro histórico de accesos que lo identifique en caso de requerirse.

5.8 Gestión de Incidencias de Seguridad Informática

Norma: El área responsable en la Unidad de TI debe mantener como política, que todos los incidentes de seguridad sobre los sistemas informáticos y redes de la Entidad, deben ser reportados al Equipo Nacional de Respuestas a Incidentes de Seguridad de la Información (CSIRT Panamá) del Estado. La Entidad cumplirá con las directrices que emita el CSIRT como parte del Plan Estratégico Nacional de Ciberseguridad.

Los objetivos principales de la Gestión de Incidentes son:

- Detectar alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio.

Justificación: Impulsar el manejo adecuado de los incidentes de seguridad en las entidades gubernamentales, para contrarrestar de manera oportuna las amenazas cibernéticas.

5.9 Seguimiento a los Contratos de Tecnología

Norma: El área responsable en la Unidad de TI debe mantener como política, el seguimiento a los contratos de TI, con el objetivo de asegurar su cumplimiento, mantener el control periódico sobre la ejecución y los acuerdos de niveles de servicio y su renovación (si aplica).

Justificación: Llevar el seguimiento de los contratos de tecnología antes, durante y después de la terminación de los mismos.

5.10 Gestión de Proyectos de TI

Norma: El área responsable en la Unidad de TI, debe prestar seguimiento a los proyectos de TI, basado en las mejores prácticas de administración de proyectos, de manera que logre el cumplimiento de los objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto preestablecidos en el caso de negocio que lo define.

Se recomienda que la entidad cuente con personal certificado en Administración de Proyectos.

Justificación: Promover la cultura de administración de proyectos para garantizar que se cumplan los objetivos esperados en el tiempo previsto y con el presupuesto asignado.

5.11 Regulaciones que afectan la gestión de TI

Norma: El área responsable en la Unidad de TI, con apoyo del Departamento Legal, debe identificar el marco jurídico y/o regulaciones que puedan afectar la gestión de TI, con el propósito de evitar posibles conflictos legales que pueden perjudicar el servicio y los activos de TI. De igual forma deberá velar por el cumplimiento del marco jurídico o las regulaciones identificadas. Podemos mencionar por ejemplo:

- Regulaciones sobre seguridad y confidencialidad,
- Disponibilidad de la información y sistemas informáticos.
- Delitos informáticos.
- Delitos relacionados con infracciones a la propiedad intelectual.

Justificación: Cumplir con las regulaciones y leyes que impactan la gestión de TI.

5.12 **Inventario General de TI**

Norma: Todas las Instituciones a través del área responsable en la Unidad de TI y la Oficina Administrativa correspondiente, tendrán la responsabilidad de realizar y mantener actualizado un inventario de todos los activos físicos de TI y de información.

El inventario debe estar organizado en dos secciones principales:

- **Activos físicos de TI (equipos)**: Donde se registrarán todos los equipos de la infraestructura TI, estaciones de trabajo, portátiles y demás.
- **Activos de programas, aplicaciones y licenciamiento**: Donde se registrarán todos los programas utilizados, sistemas operativos, bases de datos y demás.

Justificación: Impulsar el control de los activos tecnológicos en las instituciones.

6 De la Unidad de TI

6.1 Estructura de la Unidad de Tecnología de la Información en las entidades del Estado

Norma: La estructura recomendada para las Unidad de TI, contiene las siguientes secciones: Dirección de TI, Base de Datos, Redes y Comunicaciones, Soporte Técnico, Análisis y Desarrollo, Seguridad de Sistemas y la Mesa de Servicios o Mesa de Ayuda, Innovación Tecnológica. En ausencia de una oficina en la Entidad, que administre el tema de Procesos y Proyectos, la administración de TI debe contar con un área que maneje estos temas.

Justificación: Es necesaria una estructura básica en las Oficinas de Tecnología para dar soporte a los sistemas utilizados en la Entidad.

6.2 Funciones en las Dependencias de Tecnología de la Información

Norma: Debe existir una descripción del cargo para cada miembro de la Unidad de TI, y los funcionarios deben tener pleno conocimiento del mismo.

Justificación: Los funcionarios deben tener claramente definidas sus responsabilidades para la correcta gestión de los sistemas y los resultados de los componentes de Gobierno Digital que utiliza la Entidad.

6.3 La Información como Activo

Norma: La información es considerada un activo del Estado. La Entidad es responsable por el resguardo de los activos de información: bases de datos, archivos, sistemas informáticos, programas, redes y comunicaciones. Se debe asignar un propietario y/o custodio del activo. La Unidad de TI coordinará esta labor.

Justificación: Protección y buen uso de la información custodiada y almacenada por las entidades del Estado.

6.4 Comunicación y explicación de las Normas Generales de TIC

Norma: Los funcionarios deben conocer las Normas Generales correspondientes a su posición, y recibirlas de manos de la Gerencia, Dirección u Oficina Institucional de Recursos Humanos. Con el apoyo de la Unidad de TI, cada funcionario debe asistir a una charla explicativa sobre la Norma, durante el periodo de inducción y firmar un registro que compruebe su asistencia a la actividad.

Justificación: Conocimiento del marco regulatorio en materia de TI, por parte de nuevos y actuales funcionarios.

6.5 Capacitación a funcionarios, en temas de Tecnología de la Información

Norma: La Unidad de TI con el apoyo de la Gerencia, Dirección u Oficina Institucional de Recursos Humanos, debe programar capacitaciones permanentes para actualizar a los funcionarios en temas concernientes a las TIC, además de reforzar el tema de la responsabilidad de los funcionarios en general con relación a la seguridad de la información.

Justificación: Impulsar la capacitación en materia de las TIC para el desarrollo de competencias de los funcionarios para el cumplimiento de sus responsabilidades.

6.6 Normas Internas de uso de las TIC

Norma: Es responsabilidad del Jefe de la Unidad de TI, la gestión de las normas Internas de uso de las TIC, y deben estar en concordancia las presentes Normas.

Justificación: Establecer las normas de las TIC a las cuales se debe dar seguimiento y auditorías para el aseguramiento de su implementación.

6.7 Revisión de cumplimiento

Norma: La gestión de riesgos, los procedimientos de seguridad y los controles en las operaciones de TI, serán evaluados por lo menos una vez al año por personal certificado de la AIG, quien coordinara con los Gerentes, Directores o Jefes de las Gerencias, Direcciones u Oficinas de Tecnología de la información (TI), esta actividad.

Justificación: Asegurar del cumplimiento de las normas regulatorias en las operaciones de tecnología en las instituciones para la mitigación de riesgos informáticos.

7 Autorizaciones

7.1 Solicitud de Servicios a la Unidad de Tecnología de la Información

Norma: Toda solicitud de Servicio TIC, debe contar con la aprobación del director del área u oficina, antes de iniciar su trámite ante la Unidad de TI.

El Jefe de la Unidad de TI o la persona a quien él designe evaluará la solicitud para su aprobación, ejecución y documentación, o rechazo, en cuyo caso hará las observaciones necesarias a la Unidad solicitante.

Justificación: Mantener un control de las solicitudes de servicios debidamente sustentados al área de tecnología, para referencia futura y requerimientos de auditoría interna.

7.2 Inspección de archivos en dispositivos institucionales

Norma: En la circunstancia de requerir la inspección del contenido de archivos en dispositivos de la Entidad, el Jefe del área u oficina en la que se encuentra asignado un dispositivo, elevará la solicitud al Jefe de la Unidad de TI, quien autorizará al personal de Soporte Técnico para esta labor. En el caso de que la Unidad de TI sea la que necesite realizar la inspección, notificará al Jefe del área u oficina relacionada a la actividad.

Justificación: Mantener la confidencialidad de la información almacenada en los equipos dispositivos institucionales y establecer los protocolos de autorización.

7.3 Traslado de dispositivos TIC

Norma: Los dispositivos TIC, tales como: servidores, módems, equipos de comunicaciones, no deben ser trasladados sin autorización de la Unidad de TI, adicional de cumplir con los procedimientos establecidos por la oficina de Bienes Patrimoniales.

Justificación: Prevenir daño o pérdida de dispositivos y mantener la información de la ubicación de los mismos.

7.4 Privilegios o Controles de acceso a los datos

Norma: Se deben definir los privilegios de acceso a la red de la Entidad, en base a las tareas que desempeñen los funcionarios.

Justificación: Minimizar el riesgo de accesos no autorizados.

7.5 Privilegios y derechos de usuarios en Servidores y Sistemas Institucionales

Norma: Debe establecerse un procedimiento para realizar las asignaciones y privilegios de los funcionarios que tengan acceso a los Servidores y Sistemas. En caso de que el funcionario no labore en la Unidad de TI, las solicitudes deben ser gestionadas por el jefe del funcionario al Jefe de la Unidad de TI.

Los accesos deben ser auditados periódicamente por el funcionario a cargo de seguridad informática de la entidad.

Justificación: Implementar mayor seguridad en el acceso a los Servidores y Sistemas y promover la ejecución de auditorías.

8 Gestión de Licencias

8.1 Adquisición de programas informáticos

Norma: El área responsable en la Unidad de TI, es la unidad competente para realizar las recomendaciones, evaluaciones y controles, para la adquisición de programas, aplicaciones y sistemas, a lo interno de la Entidad. La Dirección u Oficina solicitante, es la responsable de sustentar la necesidad del bien o servicio ante la Unidad de TI.

Las solicitudes deben ser aprobadas por la Unidad de TI y éstas deben cumplir con lo establecido en las leyes de contrataciones públicas y las normativas del Sistema de Evaluación de Solicitudes (SES) de la AIG. Adicionalmente la Unidad de TI, debe asegurar que la iniciativa esté consignada en la Agenda Digital Institucional y en el Plan de Sistemas que se somete ante la AIG, salvo trate de una situación excepcional.

Justificación: Con el objeto de contar con la debida arquitectura, interoperabilidad y uso eficaz de las TIC en la Entidad es conveniente contar con una sola unidad autorizada, con competencias para la evaluación de adquisición de los programas, aplicaciones, sistemas en cada Entidad.

8.2 Derechos de Propiedad Intelectual sobre aplicaciones del Estado

Norma: Todas las aplicaciones, sistemas o paquetes desarrollados a la medida para las entidades por parte de empresas contratadas o de funcionarios en ejercicio de sus funciones, se consideran "Propiedad Intelectual del Estado" y la licencia de uso deberá ser perpetua. Estas pautas deberán constar en el Pliego de Cargos y en el Contrato, así como también se documentará las excepciones que se establezcan.

Todos los activos de información deben ser gestionados y monitoreados por la Entidad responsable de su custodia e inventariados para su correspondiente registro de la Propiedad Intelectual a favor del Estado.

La entidad debe solicitar el registro de dicha propiedad intelectual ante la Dirección correspondiente, en el Ministerio de Comercio e Industrias.

Justificación: Para el aseguramiento de la continuidad operativa de la Entidad es necesario que el Estado sea el Propietario Intelectual de todo desarrollo de aplicaciones y sistemas informáticos hechos a la medida de los requerimientos institucionales, en concordancia con la **Guía de Buenas Prácticas para la Adquisición de Bienes y Servicios TIC** emitida por la AIG.

8.3 Instalación de programas informáticos

Norma: Al momento de solicitar la asignación equipos para los funcionarios, el Jefe de la oficina solicitante, debe indicar a la Unidad de TI, si se requiere algún programa o aplicación especial por motivos de las tareas del funcionario.

Justificación: Mantener un control de las instalaciones y el uso de los programas informáticos que existan en la Entidad.

8.4 Comprobación de los programas informáticos

Norma: La Unidad de TI, debe implementar un mecanismo de verificación, a fin de realizar inspecciones aleatorias a los equipos, con la finalidad de identificar las aplicaciones no autorizadas. Se recomienda realizar las verificaciones mensualmente.

Justificación: Asegurar el cumplimiento de la Ley de Derecho de Autor y verificar el inventario de programas y aplicaciones instaladas.

8.5 Evidencia de adquisición de los programas informáticos

Norma: Cuando se adquiera un programa o aplicación, se debe asegurar que el proveedor sea un distribuidor autorizado. Toda la documentación que sustente la adquisición del software (copia de factura de compra, licencias y los medios de almacenamiento), debe ser custodiada por el área responsable en la Unidad de TI, de modo que es su responsabilidad mantenerla inventariada, segura, ordenada y actualizada

Justificación: Aseguramiento de la evidencia accesible y actualizada, que respalde los programas instalados en los equipos de la Entidad.

8.6 Catálogo de las Licencias de los programas informáticos

Norma: El área responsable en la Unidad de TI, debe mantener un catálogo de los programas informáticos adquiridos y debe actualizar la información de referencia:

- **Licenciante y Distribuidor**

  Es el que provee el software y su licencia. El Distribuidor es la persona jurídica a la cual la propietaria de los derechos, le otorga la facultad de distribución del software.

- **Garantía de Titularidad**

  Es la garantía ofrecida por el licenciante o propietario, en la cual, asegura que cuenta con suficientes derechos de explotación sobre el software como para permitirle proveer una licencia al licenciatario.

Justificación: Establecer al responsable de la administración del licenciamiento de los programas informáticos en la Entidad.

8.7 Actualizaciones para verificación de los programas informáticos y aplicaciones

Norma: Se recomienda que la Entidad suscriba contratos para las actualizaciones de las aplicaciones y herramientas operativas, los cuales deben incluir por lo menos dos revisiones de seguimiento al año, para evitar el vencimiento y la gestión tardía de los contratos, de conformidad con la legislación de que regula la contratación pública.

Justificación: Esta norma intenta mantener los activos tecnológicos actualizados para renovaciones oportunas que garanticen la continuidad de la operación de la Entidad, así como racionalizar la inversión sobre aquellos programas que requieran darse de baja al no tener óptima utilización.

9 Aplicaciones

9.1 Incorporación de seguridad, al ciclo de vida del desarrollo de aplicaciones

Norma: El aspecto de seguridad debe ser considerado por los diseñadores y/o desarrolladores, desde la etapa del diseño hasta la implementación (o producción). Esto quiere decir, que como parte integral del desarrollo de sistemas, deben ser incorporados controles automatizados de seguridad. Para tal efecto se recomienda seguir las siguientes acciones:

- Para cada nuevo desarrollo o mantenimiento a aplicaciones existentes, los Supervisores de Desarrollo y Seguridad Informática, deben ajustarse a lo solicitado por los usuarios funcionales, los cuales deben definir los aspectos de seguridad y accesos que requiere la aplicación. Esto debe ser indicado en la etapa del análisis.
- Los Programadores deben definir los controles de seguridad técnicos que están relacionados al sistema operativo, lenguajes de programación y facilidades de comunicación.
- El Supervisor de Seguridad, debe verificar la implementación de los controles definidos durante la etapa de diseño y establecer un esquema de verificación sobre vulnerabilidades de componentes utilizados al momento del desarrollo.

Justificación: Requerir que el grupo técnico considere el aspecto del aseguramiento de la seguridad informática como una parte fundamental en el ciclo de vida de desarrollo de sistemas y que realice verificaciones ante alertas de vulnerabilidades de parte de los proveedores y el CSIRT.

9.2 Dependencia de la seguridad de otros sistemas de información

Norma: Se deben establecer controles, en las aplicaciones que efectúen transferencias de datos entre sistemas internos o externos. La seguridad de un sistema de información no debe depender enteramente de la seguridad establecida en otros sistemas. Se debe filtrar la información que proviene de los sistemas externos y asegurarse que los datos a ingresar a las aplicaciones de la entidad sean lo más confiables posible.

Justificación: Comprometer a los diseñadores y otros miembros del equipo técnico, a considerar la inclusión de mecanismo de seguridad en los sistemas.

9.3 Documentación de la operación y entrenamiento de la aplicación

Norma: Una aplicación no debe ser pasar a la condición de "producción", si no cuenta con los manuales de usuario, de administración y operación del mismo.

Justificación: Esta norma procura que toda la documentación del sistema sea preparada y aprobada, antes que el sistema entre en producción.

9.4 Convenciones para el desarrollo de sistemas

Norma: El Supervisor de Desarrollo y los Programadores, deben adoptar metodologías, guías de estilo o patrones de diseño, para el desarrollo de aplicaciones, asegurando que todo el desarrollo mantenga uniformidad y así, el conjunto total es visto y comprendido como coherente y vinculado.

Justificación: Lograr uniformidad en la forma como se desarrollan las aplicaciones.

9.5 Avisos de fallas en las aplicaciones desarrolladas y su operación

Norma: Cuando una aplicación falla en una operación o que la misma no se realice correctamente (errores en tiempo de ejecución o errores lógicos), el sistema o la aplicación debe presentar un código de error acerca del fallo.

Justificación: Identificar los errores de los programas para que se tomen medidas adecuadas al respecto.

9.6 Calidad de las aplicaciones

Norma: Para la comprobación de la calidad de las aplicaciones, se recomienda utilizar el estándar ISO/IEC 25000 SQuaRE (Software Product Quality Requirements and Evaluation) vigente, el cual cubre dos procesos principales: La especificación de requisitos de calidad del software y la evaluación de la calidad del software, soportada por el proceso de medición de calidad del software.

Contenido de la norma:

- Términos y definiciones
- Modelos de referencia
- Guía general
- Guías por división
- Estándares internacionales para especificación de requerimientos, planificación y gestión, medición y evaluación de la calidad del producto.

9.7 Pruebas a las aplicaciones

Norma: Es una actividad del proceso de control de calidad, cuyo objetivo es proporcionar información objetiva e independiente sobre la calidad del producto. Las pruebas son básicamente un conjunto de acciones dentro del desarrollo de software.

En la medida de las posibilidades se debe realizar estas pruebas a las aplicaciones desarrolladas o adquiridas.

Los tipos de pruebas más conocidos son:

- Pruebas funcionales
- Prueba de aceptación
- Prueba de la instalación
- Prueba de integración
- Prueba de regresión
- Prueba de humo
- Prueba de desempeño
- Prueba de carga
- Prueba de estrés
- Prueba de volumen
- Prueba de usabilidad
- Prueba de campo
- Prueba de recuperación y tolerancia a fallas
- Prueba de seguridad y control de acceso

Se recomienda que el personal involucrado en la labor de desarrollo de aplicaciones, no realice las pruebas funcionales o finales, ni se involucre en la operación día a día de esa aplicación. Si existieran facilidades que lo permitan, todas las pruebas formales deben ser realizadas por funcionarios especializados y con el acompañamiento de los usuarios finales.

Justificación: Verificar que se cumplan con las especificaciones planteadas y asegurar que el trabajo realizado cumple en cuanto a la calidad y desarrollo seguro.

9.8 Ambientes separados para desarrollos, pruebas y producción

Norma: Las aplicaciones en desarrollo deben mantenerse estrictamente separadas de la aplicación en producción. Se recomienda, si existen facilidades que lo permitan, la separación física de ambos ambientes (desarrollo y producción). Cuando no se tiene esta facilidad, se deben separar los archivos en directorios, librerías, otros, empleando controles de acceso estrictos, es decir, niveles de seguridad mínimos para evitar el acceso de los programadores a los datos en producción.

Justificación: Impulsar la separación y el establecimiento de medidas de control interno para minimizar riesgos de accesos no autorizados en los sistemas en producción.

9.9 Control de versiones en los Desarrollos

Norma: En el caso de existir una estructura para el desarrollo de programas o aplicaciones en la entidad, se recomienda la implementación de un control para las versiones, manteniendo un registro de evolución adecuado que permita restaurar a la instancia anterior en caso de fallas.

Justificación: Mantener un control de actualizaciones de los sistemas en producción.

10 Adquisición y mantenimiento de la Infraestructura tecnológica

10.1 Recomendación, evaluación y controles para la adquisición de hardware

Norma: El área responsable dentro de la Unidad de TI estará a cargo de efectuar las recomendaciones, evaluaciones y controles en la adquisición de bienes y servicios tecnológicos, dentro de la Entidad. Adicional, deben cumplir con la normativa del SES y asegurarse que la iniciativa esté registrada en la Agenda Digital Institucional y en el Plan de Sistemas entregado a la AIG.

Justificación: Para el manejo integral de los dispositivos y software en las Entidades, se requiere de una sola instancia actué como ente, responsable y encargado de la evaluación de los bienes y servicios tecnológicos dentro de las Entidades.

10.2 Guías y Estándares Tecnológicos

Norma: El área responsable en la Unidad de TI de la Entidad debe utilizar las guías y recomendaciones sobre los Estándares autorizados por la AIG, al momento de la adquisición de bienes o servicios informáticos y sobre la base de su Plan de Sistemas.

Se recomienda que toda adquisición de tecnología, se realice o analice, a través de un Comité conformado por personal de la Unidad de TI y el Director de la Unidad u Oficina solicitante de los bienes o servicios informáticos.

El área responsable al momento de planificar las actividades de adquisición de bienes informáticos, debe establecer las prioridades. Referirse a la Guía para la Obtención del Concepto Favorable de la AIG vigente, para la Contratación de Bienes o Servicios de TIC.

Justificación: Utilizar normas y procedimientos para la adquisición de bienes y servicios de tecnología en la Entidad, basado en el Plan de Sistemas de la Oficina de TI, asegurar la sostenibilidad e interoperabilidad de las soluciones a ser contratadas.

10.3 Actualización de hardware

Norma: El área responsable en la Unidad de TI debe realizar una revisión anual que incluirán las recomendaciones relacionadas a la actualización o reemplazo del hardware.

Justificación: Actualización para la operatividad de los sistemas y reducción de riesgos informático.

10.4 Cableado Estructurado y redes Inalámbricas

Norma: El área responsable en la Unidad de TI debe asegurarse que se cumpla lo recomendado por la AIG, en referencia a las Normas y Estándares Internacionales sobre Cableado Estructurado, las que regulan las especificaciones para el diseño, construcción, instalación, administración y mantenimiento de las redes de comunicación. De la misma manera deben contemplarse las redes inalámbricas en todas sus versiones, bandas y frecuencias (IEEE 802.XXX, WiFi, Bluetooth, etc.), manteniendo la debida configuración, restricción, acceso y seguridad apropiada.

Justificación: Garantizar la correcta operación de los servicios de telecomunicación aplicando las normas para redes de comunicaciones que recomiende la AIG.

10.5 Contratación de terceros para la implementación y mantenimiento

Norma: De no contar la Entidad con el recurso humano capacitado para realizar los procesos de implementación o mantenimiento de la infraestructura tecnológica y se opte por recurrir a la contratación de terceros, se recomienda establecer un Manual o Guía para el desarrollo de los "Términos de Referencia" (TDR), que incluya las especificaciones técnicas y los requisitos o condiciones requeridas o aplicables.

Asimismo, se establecerán los criterios, términos y pruebas de aceptación de lo contratado. Además de establecer en el contrato aquellas cláusulas que establezcan la forma en que la empresa contratada, realizará la Transferencia de Conocimiento Tecnológico sobre la materia objeto de contratación, con el objetivo de minimizar la dependencia de la entidad respecto a terceros.

La Unidad de TI debe incluir en el contrato, las especificaciones, requisitos o condiciones requeridas o aplicables a la contratación de terceros.

Se recomienda utilizar como referencia la Guía para La Obtención del Concepto Favorable de la AIG vigente para la Contratación de Bienes o Servicios de TIC.

Justificación: Aseguramiento de la calidad del entregable contratado y su sostenibilidad.

10.6 Elaboración y prueba de los procedimientos de TI

Norma: Las actividades y servicios que realiza la Unidad de TI, (respaldo de datos, configuración de servidores, corrección de errores, instalación de software crítico, mesa de ayuda, otros), deben de contar con un procedimiento para su realización. Todo procedimiento debe ser sometido a un proceso de verificación o prueba y de ser posible, lo efectúe la oficina de auditoria interna o en su defecto por un grupo multidisciplinario.

Justificación: Garantizar la creación, documentación y verificación de los procedimientos técnicos de TI.

10.7 Aprobación de los procedimientos de TI

Norma: Los procedimientos de TI, tales como las políticas, estándares, mejores prácticas y guías, deben ser revisados por un Comité Técnico de la Unidad de TI y aprobados por el Comité de Procedimientos de la Entidad, de contar con esta instancia o similar.

Justificación: Garantizar que los procedimientos de Tecnología puedan ser auditables.

10.8 Documentación de los procedimientos de TI

Norma: Los Manuales de Procedimientos de TI deben ser elaborados por los miembros de la Unidad de TI y deben mantenerse actualizados y en versión digitalizada, disponible al usuario autorizado. Para la documentación de los procedimientos catalogados como críticos, recomendamos se conserve una copia digitalizada fuera de la entidad.

Justificación: Salvaguardar y mantener accesibles los procedimientos de Tecnología.

11 Procedimientos en TI

11.1 Elaboración y prueba de los procedimientos de TI

Norma: Las actividades y servicios que realiza la Unidad de TI, (respaldo de datos, configuración de servidores, corrección de errores, instalación de software crítico, mesa de ayuda, otros), deben de contar con un procedimiento para su realización. Todo procedimiento debe ser sometido a un proceso de verificación o prueba y de ser posible, lo efectúe la oficina de auditoria interna o en su defecto por un grupo multidisciplinario.

Justificación: Garantizar la creación, documentación y verificación de los procedimientos técnicos de TI.

11.2 Documentación de los procedimientos de TI

Norma: Los Manuales de Procedimientos de TI deben ser elaborados por los miembros de la Unidad de TI y deben mantenerse actualizados y en versión digitalizada, disponible al usuario autorizado. Para la documentación de los procedimientos catalogados como críticos, recomendamos se conserve una copia digitalizada fuera de la entidad.

Justificación: Salvaguardar y mantener accesibles los procedimientos de TI.

11.3 Aprobación de los procedimientos de TI

Norma: Los procedimientos de TI, tales como las políticas, estándares, mejores prácticas y guías deben ser revisados por un Comité Técnico de la Unidad de TI y aprobados por el Comité de Procedimientos de la Entidad, de contar con esta instancia o similar.

Justificación: Garantizar que los procedimientos de Tecnología sean oficiales y puedan ser auditables.

12 Administración de los Mantenimientos en los Sistemas

12.1 Instalación de actualizaciones

Norma: La aplicación de actualizaciones, parches o mejoras a los equipos servidores y aplicaciones en producción, es una responsabilidad directa de los Supervisores de TI. Se recomienda que sean aplicados en un ambiente de pruebas, antes de ser implementados en los equipos en producción y deben contar con una autorización por escrito para poder ser aplicadas en el ambiente de producción o en los equipos. Debe establecerse la documentación del Control de estas actualizaciones.

Justificación: Garantizar que las actualizaciones y parches se apliquen una vez concluya a satisfacción el proceso de prueba y autorización.

12.2 Los cambios a las aplicaciones deben ser parte de un procedimiento formal

Norma: Debe existir un procedimiento formal y por escrito para la gestión de las solicitudes de cambios en las aplicaciones.

Justificación: Requerir el uso de un procedimiento formal y escrito, para el control del cambio de las aplicaciones en producción.

12.3 Autorización de cambios directos a los datos en producción

Norma: Para modificar los datos en producción, en el caso que se requiera corregir una inconsistencia, el Gerente o Director del área afectada debe solicitar formalmente al área técnica responsable de TI, su rectificación. La ejecución de las tareas de corrección debe efectuarse con la participación de personal de auditoría interna y el supervisor de seguridad, quien debe autorizar el rol en el ambiente de producción por el tiempo que demore la corrección de acuerdo a los procedimientos establecidos. Se debe mantener en respaldo los datos antes y después de la corrección. Si el problema es recurrente debe automatizarse la funcionalidad y asignarla al usuario final autorizado.

Justificación: Proteger la integridad de datos en producción.

12.4 Bitácora de cambios y actualizaciones

Norma: El área responsable en la Unidad de TI debe establecer una bitácora para el registro de todas las actualizaciones, mejoras o parches que sean instalados en los Aplicativos o Sistemas Informáticos.

Justificación: Control de las instalaciones y actualizaciones del sistema o aplicativos, con la finalidad de contar con las pistas de auditoría.

12.5 Documentación de las modificaciones realizadas a la aplicación

Norma: Se debe mantener la documentación que refleje todos los cambios significativos a la aplicación y debe ser actualizada inmediatamente después de ser implantados los cambios.

Justificación: Mantener correctamente documentados el origen o sustento de los cambios a las aplicaciones y asegurar las recuperaciones por desastres parciales o totales.

12.6 Acceso del personal de desarrollo al ambiente en producción

Norma: El personal que participa en el desarrollo de programas o sistemas, no debe tener acceso a los sistemas en producción.

Justificación: Mantener la integridad y seguridad de la información en producción.

12.7 **Comunicación de cambios en la Tecnología de Información**

Norma: El área responsable en la Unidad de TI y/o la Gerencia o Dirección de Procesos y Mejoras Continua de cada entidad, es la responsable de comunicar oportunamente a los usuarios finales y con suficiente antelación, los cambios que se realizarán a la plataforma tecnológica, siempre y cuando estos cambios afecten a los servicios que ofrece la Entidad.

Justificación: Asegurar que los funcionarios internos y externos sean informados de los cambios que se realicen en la plataforma tecnológica y de los efectos que estos cambios podrían tener, en las operaciones de los servicios brindados por la Entidad.

12.8 **Identificación de errores o problemas en los sistemas o aplicaciones**

Norma: Cuando algún funcionario identifique una falla, error o se presente un problema en los sistemas y/o aplicaciones, éste debe reportarlo al personal de la mesa de ayuda o personal de soporte técnico designado. El personal de la mesa de ayuda, se encargará de tomar las medidas necesarias para su solución según el procedimiento utilizado.

Justificación: Contribuir a la depuración y mejora de los sistemas o aplicaciones de manera controlada.

13 Niveles del servicio interno y relaciones con terceros

13.1 Primer nivel de servicio a los funcionarios

Norma: El primer nivel de servicio que los funcionarios reciben, es a través del personal de la Mesa de Servicios o Mesa de Ayuda de la Unidad de TI o mediante servicio contratado a terceros, quienes se encargarán de brindarles soporte y ayuda en los aspectos técnicos y de procedimientos. En caso que la solución a la solicitud del funcionario esté fuera del alcance de este nivel, el requerimiento será transferido al segundo nivel de servicio.

Justificación: Informar a los funcionarios el alcance del primer nivel de servicio con que cuentan.

13.2 Segundo nivel de servicio a los funcionarios

Norma: El segundo nivel de servicio, está bajo la responsabilidad del personal de Soporte Técnico especializado de la entidad, en compañía del Supervisor de Soporte de ser necesario.

Justificación: Informar a los funcionarios el alcance del segundo nivel de servicio con que cuentan.

13.3 Tercer nivel de servicio a los funcionarios

Norma: El tercer nivel de servicio para los funcionarios en caso que las solicitudes no puedan ser atendidas por el personal de Soporte Técnico especializado, recaerá sobre los proveedores externos de las soluciones tecnológicas de la entidad.

Justificación: Informar a los funcionarios el alcance del tercer nivel de servicio con que cuentan.

13.4 Cláusula de confidencialidad

Norma: Todo Contrato realizado con proveedores, especialistas o contratistas debe incluir una Cláusula de Confidencialidad, en donde el proveedor se comprometa a resguardar la confidencialidad de la información a la que tenga acceso, salvaguardando los intereses de la entidad.

Justificación: Establecer el compromiso de confidencialidad entre el Contratista y la Entidad que permita salvaguardar la información de la Entidad.

13.5 Administración de los bienes del Estado, utilizados por terceros

Norma: Los bienes tecnológicos propiedad del Estado que vayan a ser utilizados por contratistas, proveedores o especialistas de la Entidad, deben ser asignados y controlados por el personal de TI. Se debe instaurar un procedimiento y un cronograma de revisión.

Justificación: Mantener un control estricto de los bienes que pertenecen al Estado y que estén siendo utilizados por terceras personas.

13.6 Devolución de los bienes del Estado al término de un Contrato

Norma: En el momento que todo proveedor, especialista, o contratista culmine su relación con la Entidad y que utilice o tenga acceso a bienes tecnológicos propiedad del Estado o sus facilidades, estos deben ser reintegrados a la Entidad o restringidos. Estos bienes o activos incluyen: dispositivos, libros, documentación, manuales, llaves, tarjetas o claves de acceso a

facilidades entre otros. Se debe reintegrar a la Administración toda propiedad que posean, así como también todos los privilegios en los sistemas computacionales, los privilegios del acceso físico, y otros privilegios que se les haya otorgado. El Jefe de la Unidad de TI, asegurará la debida documentación de los bienes asignados y supervisará esta labor.

Justificación: Recuperar toda pertenencia la cual se tuvo acceso, además del controlar los derechos y privilegios en los sistemas de información del Estado para salvaguardar los bienes e información del Estado.

13.7 **Conexión a la red local de la Entidad, con equipos tecnológicos de terceros**

Norma: En el caso de que los proveedores u otros, deban utilizar equipos provistos dentro de la red de la Entidad deben solicitar por escrito o vía correo electrónico al área responsable en la Unidad de TI, la fecha y la hora en que estarán en las instalaciones, para tomar las previsiones necesarias siguiendo los acuerdos de confidencialidad.

Justificación: Controlar la introducción de equipos no perteneciente a la Entidad (en este caso de los proveedores) y evitar inconvenientes con el personal de seguridad y demás consideraciones para salvaguardar la información del Estado.

13.8 **Utilización de Internet de la entidad, por parte de proveedores o visitantes**

Norma: Aquellos proveedores que por motivo de sus tareas con la entidad necesiten acceso a Internet, deben enviar al área responsable en la Unidad de TI y con suficiente antelación a la fecha de inicio de su trabajo, una nota donde soliciten se les autorice este acceso y el tiempo que van a necesitar estar conectados al Internet. La conexión para proveedores o visitantes debe realizarse a través de la red de invitados.

Justificación: Evitar que cualquier proveedor o visitante tenga acceso a Internet sin una autorización previa del área responsable de la Unidad de TI, lo cual es una buena práctica de seguridad.

14 Continuidad del servicio

14.1 Gestión de la Continuidad de los Servicios TI

Norma: El área responsable en la Unidad de TI, debe adoptar una metodología para la Gestión de la Continuidad del Servicio de TI, para lo cual recomendamos consideren el punto 4.6 **Gestión de la Continuidad de Servicios de TI** (ITSCM) dentro del 2do. Libro Diseño del Servicio de la Biblioteca de Infraestructura de Tecnologías de Información (ITIL) en su versión vigente.

Subsiguientemente puede adoptar la Norma ISO/IEC 27031: Guías para la preparación de las tecnologías de información y comunicaciones para la continuidad del negocio, en su versión vigente.

Justificación: Prevenir y gestionar los acontecimientos imprevistos y/o desastres naturales u otras fuerzas de causa mayor que afecten los Servicios de TI.

14.2 Preparación y mantenimiento de un Plan de Contingencia

Norma: La Entidad debe poseer un Plan de Contingencia para la continuidad de su operación, en la medida de sus posibilidades, en donde se establece la estructura estratégica y operativa para gestionar situaciones de emergencia sobre las plataformas críticas previamente identificadas. El Plan debe documentar los procedimientos a realizar en caso de interrupciones en las operaciones tecnológicas. El Plan debe ser actualizado periódicamente y debe ser probado como mínimo una vez al año.

Justificación: Contar con mecanismos alternos y de redundancia para mantener la operación de la Entidad y el servicio a los usuarios.

14.3 Implementación de un Plan de Recuperación de Desastres

Norma: Para la implementación del Plan de Recuperación de Desastres (DRP), se recomienda completar los siguientes pasos:

- Inventario de aplicaciones y su criticidad.
- Identificación de riesgos.
- Escenario de desastres.
- Prioridades y costos.
- BIA (análisis de impacto al negocio).
- RTO (objetivo de tiempo de recuperación).
- RPO (objetivo de punto de recuperación).
- Determinar la infraestructura requerida.
- Plan de comunicación.
- Procedimientos para mitigar y asegurar la continuidad de la operación.
- Establecer el equipo humano responsables según la emergencia con roles y niveles de aprobación.
- Pruebas.

Justificación: Establecer los pasos mínimos aplicables para ejecutar el DRP.

14.4 Condiciones de las salas de servidores

Norma: El área que hospeda los servidores y equipos de comunicación, debe tener un ambiente controlado que ayude a detectar y disminuir la ocurrencia de eventos que puedan afectar el ambiente requerido, así como debe estar ubicado en áreas resguardadas, alejadas de fuentes de suministro de agua o aspersores de agua contra incendios que puedan afectar los equipos de informática y tecnológicos.

Para ello debe contar con los siguientes sistemas o tecnologías:

- Sistema de protección y detección de incendios (sensores de humo, alarma contra incendio, extintores, sistema de supresión de fuego especializado para equipo informático), el cual debe enviar una notificación alertando sobre este evento al cuerpo de bomberos más cercano y al personal de tecnología designado.
- Sistema de control de humedad (detector de humedad, detector de agua) el cual debe enviar una notificación alertando sobre estos eventos al personal de tecnología designado.
- Equipos para monitorear otros factores tales como: temperatura, voltaje, amperaje, que puedan enviar alertas vía red local, correo electrónico o mensajes cortos (SMS), alertando sobre estos eventos al personal de Tecnología designado.
- Contar con Unidad de Poder Secundario y Planta Eléctrica.

Justificación: Establecer los mecanismos de previsión y alerta con los que debe contar el área de servidores y equipos de comunicación.

14.5 Protección de los equipos contra condiciones eléctricas

Norma: Todos los equipos computacionales deben estar habilitados con dispositivos para protección de descargas eléctricas. La sala de servidores debe estar provista con conexiones a tierra para absorber las descargas eléctricas. Estas adecuaciones deben ser supervisadas por el área responsable en la Unidad de TI.

Justificación: Asegurar que las posibles descargas eléctricas no causen daños a los dispositivos TIC y que estén protegidos para prevenir pérdidas de datos.

14.6 Respaldo de Información

Norma: Toda la información clasificada como confidencial, crítica y cambiante, debe ser respaldada diariamente. Se recomienda que la información de menor nivel de confidencialidad y que no sufre cambios, se respalde como mínimo semanalmente. Los períodos de respaldo deben ser proporcionales al nivel de criticidad de la información y dichos respaldos deben ser verificados. Para evitar que el procedimiento de respaldo sea ineficiente, se recomienda que este proceso se automatice.

Justificación: Minimizar el riesgo de pérdida de datos y aumentar las posibilidades de recuperación.

14.7 Proyectos de misión crítica, redundancia y alta disponibilidad

Norma: Para las aplicaciones de misión crítica, la Entidad debe incorporar los conceptos de redundancia y alta disponibilidad en los servidores, equipos de comunicación y redes. Las medidas a implementar deben contemplar el monitoreo de los sistemas para aumentar la

capacidad en la detección de fallas y recuperación de incidentes, afectando lo menos posible el servicio.

Justificación: Asegurar la operación y funcionamiento de los proyectos críticos de la Entidad frente a algún evento imprevisto.

15 Normas de aplicación en los equipos servidores

15.1 Control de acceso al cuarto de servidores

Norma: Todo el personal, sea funcionario, soporte técnico externo o visitante, que requiera acceso al área donde están alojados los servidores, debe estar explícitamente autorizado por el área responsable en la Unidad de TI y firmar un registro físico.

Si no es personal de la entidad, el visitante debe estar acompañado por personal de tecnología, el cual se encargará de supervisar su estadía dentro del área y se asegurará que firme el registro de entrada y salida.

Justificación: Controlar el personal que ingrese al área de servidores para trazabilidad y protección de los activos e información.

15.2 Privilegios en los Servidores

Norma: Se controlará y limitará el acceso lógico y privilegios a los funcionarios de TI que utilicen los servidores mediante un protocolo establecido. En caso de que requieran ser accedidos por proveedores, se definirán usuarios temporales específicos con privilegios apropiados y con la debida caducidad y trazabilidad de los mismos. Los accesos deben ser auditados periódicamente por el administrador de seguridad.

Justificación: Implementar mayor seguridad al acceso lógico en los equipos servidores y reforzar el cumplimiento de las auditorías.

15.3 Administración Proactiva

Norma: El personal del área responsable en la Unidad de TI, debe velar por la disponibilidad, capacidad, desempeño y uso de las plataformas tecnológicas, verificando la correcta operación de los sistemas.

Para cumplir con esta responsabilidad, se debe realizar diariamente revisiones a los Sistemas evaluando el rendimiento y observando que no se sobrepase la capacidad de los discos duros, memoria, procesadores, entre otros aspectos.

En la medida de sus posibilidades, deben implementarse las herramientas para el monitoreo de las capacidades TIC y debe llevarse una bitácora que registre las revisiones y evaluaciones de cualquier incidente que se halla registrado.

En el caso que la Entidad haya establecido un contrato para la tercerización o subcontratación de Servicios de TI, el personal del área responsable en la Unidad de TI, debe solicitar un informe periódico de la evaluación de las plataformas tecnológicas a la empresa contratada.

Justificación: La finalidad de identificar posibles problemas antes que los mismos se presenten y así poder brindar una solución oportuna y eficaz para mantener las plataformas tecnológicas en óptimas condiciones y 100 % operativas.

15.4 Ubicación de servidores

Norma: Todos los servidores, deben estar ubicados dentro de la(s) Sala(s) de Servidores o Centro de Procesamiento de Datos y los mismos deben ser alojados en gabinetes ("racks"), estantes o anaqueles apropiados, evitando colocarlos en el suelo o en muebles no adecuados.

Justificación: Proteger los Servidores ubicándolos en las áreas especialmente habilitadas para su cuidado y funcionamiento.

15.5 **Activar bloqueo automático**

Norma: Cuando no se estén utilizando los servidores, sus pantallas deben permanecer bloqueadas con protectores de pantalla que no consuman recursos del sistema.

Justificación: Mantener la seguridad de los servidores impidiendo el acceso no autorizado.

15.6 **Recursos compartidos en servidores**

Norma: Todo recurso compartido en los servidores de archivos debe estar protegido mediante permisos de acceso. Se debe evitar definir recursos compartidos con acceso total.

Justificación: Evitar accesos no autorizados a los recursos compartidos.

15.7 **Actualizaciones**

Norma: Los servidores en producción no deben estar configurados para realizar actualizaciones automáticamente. En su defecto, se debe organizar de forma controlada la aplicación de las actualizaciones, minimizando el impacto en las operaciones.

Justificación: Evitar el impacto a la operación de la Entidad por la actualización no contralada de los servidores.

16 Administración Integral del Riesgo

16.1 Administración del riesgo tecnológico.

Norma: La Unidad de TI, en caso de no existir una oficina responsable del tema de riesgo tecnológico, debe implementar una metodología de administración de riesgo tecnológico para prevenir y responder adecuadamente a las amenazas que puedan afectar la gestión de TI. Dicha metodología debe cubrir los procesos tecnológicos y los sistemas informáticos.

Justificación: Reducir el riesgo tecnológico a niveles aceptables.

16.2 Evaluación del riesgo tecnológico

Norma: Se debe realizar una evaluación del riesgo, con base a la metodología adoptada, por lo menos una vez al año y el informe de resultados debe ser presentado a la máxima autoridad de la Entidad.

Justificación: Establecer y mantener actualizado los niveles de riesgo tecnológico, así como tomar decisiones al respecto de su estado actual.

17 Monitoreo de las bitácoras

17.1 Eventos del Sistema

Norma: Todo Sistema Operativo debe contar con una herramienta para el monitoreo y registro de la ocurrencia de los eventos del sistema operativo y principalmente los de seguridad.

Justificación: Mantener una trazabilidad y un control de los eventos de los sistemas.

17.2 Bitácoras para el manejo de información confidencial

Norma: De ser posible, y si la infraestructura tecnológica lo permite, todos los sistemas en producción que procesen información confidencial de la Entidad, deben generar un registro en bitácora al momento de realizar operaciones de inserción, modificación o eliminación de información confidencial.

Justificación: Registrar todo cambio realizado a la información clasificada como confidencial.

17.3 Período de retención de las bitácoras del sistema

Norma: Las bitácoras relacionadas a los eventos de seguridad en los sistemas, deben ser retenidas al menos por noventa (90) días. Durante este período, se debe asegurar que estas bitácoras no sean modificadas y luego del periodo indicado, deben ser almacenadas en un medio magnético y preservadas en un lugar seguro.

Justificación: Establecer la normativa para la preservación de la información de trazabilidad de los eventos de los sistemas.

17.4 Personal autorizado para la revisión de las bitácoras del sistema

Norma: Las bitácoras deben ser almacenadas de forma tal que sólo puedan ser accedidas por personal autorizado para la corrección de errores, auditorias, recuperación de la configuración y tareas relacionadas. En la medida de las posibilidades la información de las bitácoras debe estar cifrada y/o protegida mediante contraseñas. La supervisión de esta disposición es responsabilidad del Jefe de la Unidad de TI o la persona que él designe.

Justificación: Restringir el acceso a las bitácoras para proteger la información de trazabilidad de los eventos de los sistemas.

17.5 Revisión regular de las bitácoras del sistema

Norma: Se debe revisar diariamente las bitácoras monitoreando la información de los registro de eventos del sistema operativo.

La persona encargada de la revisión, debe emitir un informe o correo electrónico al Jefe del área responsable en la Unidad de TI, con los resultados de las revisiones.

Justificación: Regular la revisión de las bitácoras de los sistemas con la finalidad de identificar anomalías y eventos disruptivos.

18 Cambios en el control de acceso, por acciones de personal

18.1 Traslados de funcionarios

Norma: La Unidad de TI debe coordinar con la Gerencia u Oficina Institucional de Recursos Humanos, el establecimiento de los procedimientos a seguir al momento de producirse una acción de personal que requiera cambios en el control de acceso.

Aplicar los siguientes lineamientos:

- Informar con una anticipación apropiada, y por escrito, al Jefe de la Unidad de TI, el detalle de la nueva posición y/u oficina asignada.
- Gestionar la reasignación de las responsabilidades sobre información confidencial y/o reservada que administraba el funcionario.

La Dirección de Tecnología procederá:

- Desactivar las cuentas y permisos del funcionario en el departamento que laboraba.
- Desactivar los códigos de acceso a áreas físicas, códigos telefónicos, códigos de alarmas, así como atender los dispositivos que estuviesen a cargo del funcionario.
- Activar los nuevos accesos lógicos y físicos de su nueva posición y/u oficina.

Justificación: Coordinar las acciones a seguir y responsabilidades al momento del traslado de los funcionarios.

18.2 Retiro de funcionarios

Norma: Cuando el personal de la entidad, renuncie o sea despedido, el jefe inmediato del funcionario debe realizar las siguientes acciones:

- Informar inmediatamente al Gerente, Director o Jefe de Seguridad de la Unidad de TI, para que se proceda a la revocación a partir del momento efectivo de la renuncia o despido de todos los permisos de acceso lógico y físico que posea el individuo, incluyendo los códigos telefónicos, de alarmas, dispositivos (si aplica). Además de la desactivación de las cuentas utilizadas en las diferentes aplicaciones y herramientas.
- Exigir el retorno de todos los registros de información y dispositivos utilizados por el funcionario y que son propiedad de la Entidad.

Justificación: Proteger la información y los activos de la Entidad, previniendo acciones que pueda tomar, en especial, el funcionario destituido o cesado.

18.3 Transferencia de los deberes de custodia y gestión de documentos, al finalizar la relación laboral con el funcionario

Norma: Se recomienda que cuando un funcionario renuncie o sea despedido, los archivos almacenados en su computadora y los documentos impresos, deben ser examinados por el personal designado por el Oficial de Seguridad de la Información o en su defecto el Oficial de Seguridad Informática. Se recomienda se acompañe por personal de la Gerencia u Oficina Institucional de Recursos Humanos. El Director del área del funcionario es quien debe asignar a un nuevo responsable, en caso que exista información confidencial y/o privada que necesite ser custodiada.

Justificación: Mantener las responsabilidades de custodia de la información confidencial y/o privada, con la cual se asegura que las medidas de seguridad de la información se conserven en las condiciones mínimas aceptables.

18.4 **Vacaciones de funcionarios**

Norma: El jefe inmediato del funcionario, debe informar con antelación y por escrito, al área responsable en la Unidad de TI, el período de vacaciones del funcionario y si se requiere desactivar temporalmente las cuentas y/o códigos de accesos a los diferentes sistemas y aplicaciones.

Justificación: Minimizar el riesgo de la utilización de las contraseñas o cuentas de funcionario que se encuentra de vacaciones.

18.5 **Devolución de equipos del Estado**

Norma: Cuando se produce una acción de personal para el despido de un funcionario, o que éste renuncie, la Gerencia, Dirección u Oficina Institucional de Recursos Humanos, debe coordinar con la oficina administrativa competente, la devolución de todos los equipos tecnológicos que el exfuncionario custodie, y debe devolverlos con la información existente sin ser alterada. No debe formatear los equipos.

Justificación: Recuperar los equipos ante la terminación laboral de un funcionario y preservar la información de la Entidad, que es un activo propiedad del Estado.

19 Confidencialidad

19.1 Compromiso del Estado en la custodia de datos

Norma: La Entidad, por medio del área responsable en la Unidad de TI, debe garantizar la protección de los datos personales y la confidencialidad de la información en los sistemas informáticos, tomando las medidas necesarias para este fin, acorde a los estándares y protocolos apropiados según la naturaleza de la información, así como las leyes que regulen esta materia.

Justificación: Asegurar la protección y confidencialidad de datos, generando confianza en los usuarios de la Entidad y los ciudadanos.

19.2 Cifrado

Norma: Todos los canales de acceso a la información deben ser seguros, por lo que recomienda la utilización de cifrado, controles de autenticación e integridad criptográfica.

Justificación: Garantizar el mayor grado de seguridad en los canales de acceso de la Entidad.

19.3 Autorización para verificar los Correos Electrónicos en el Estado

Norma: Está terminantemente prohibido que el personal de Tecnología revise los correos electrónicos de la entidad asignados a los funcionarios, salvo que se cuente con la autorización por escrito del Despacho Superior o que se trate de una investigación judicial.

Justificación: Resguardar la información contenida en los correos electrónicos institucionales propiedad del Estado.

19.4 Revisión de la actividad en Internet

Norma: La Unidad de TI, autorizará al Oficial de Seguridad Informática, a examinar la actividad de los funcionarios en el Internet, solamente con el propósito de administrar los recursos y/o brindar soporte a investigaciones o auditorías.

Justificación: Normar la confidencialidad y los lineamientos para la revisión del recurso de internet.

20 Gestión del Perímetro de Seguridad

20.1 Cortafuegos (Firewalls)

Norma: Se debe implementar uno o varios dispositivos cortafuegos para la protección de ataques e intrusiones procedentes del exterior o desde el interior. Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos, permitiendo al mismo tiempo comunicaciones o tráfico autorizado sobre la base de un conjunto de normas y otros criterios.

Justificación: Bloquear el acceso no autorizado y prevención de ataques o afectaciones a los sistemas del Estado.

20.2 Sistemas de Prevención de Intrusos (IPS)

Norma: Se debe implementar un Sistema de Prevención de Intrusos (o **IPS** por sus siglas en inglés de "Intrusion Prevention System"), el cual ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. Deben contar con capacidades de protección y detección de intrusiones o actividad maliciosa de manera proactiva y reactiva, además de grabar información histórica y generar reportes.

Justificación: Prevenir el acceso no autorizado y detectar ataques o afectaciones a los sistemas del Estado.

20.3 Implementación de Cortafuegos de Aplicación

Norma: Se debe implementar un dispositivo (hardware o software), que permita proteger las aplicaciones web empleando un conjunto de reglas al tráfico HTTP/HTTPS para detectar y bloquear peticiones de diversos y específicos ataques. Los Web Application Firewalls (WAF) son elementos complementarios a las medidas de seguridad que soportan los Firewall clásicos. Los servidores Web, no son protegidos por los IDS/IPS.

Justificación: Las entidades deben contar con dispositivos con las capacidades de analizar el tráfico web y proteger las aplicaciones web de diversos ataques.

20.4 Protección del Correo Electrónico (Antispam)

Norma: Se debe implementar un sistema, servicio o software para la protección del Correo Electrónico, el cual reducirá la entrada de mensajes de correo no deseados (spam) y filtrara los mensajes de correo que contengan virus.

Justificación: Mantener el Servicio de Correo lo más seguro posible y mantener disponible los recursos de mensajería al usuario.

20.5 Filtrado de Contenido Web (Web Filter)

Norma: Se debe implementar un sistema de filtro de contenido para restringir el acceso del funcionario a ciertos sitios de la *Web*. La implementación puede ser de tipo software o hardware mediante un dispositivo o "appliance."

Justificación: Hacer buen uso de los recursos de información Web disponible a los funcionarios.

20.6 **Protección contra Ataques de Denegación de Servicio (DoS - Denial of Service DDoS - Distributed Denial of Service)**

Norma: Contar con un plan de acciones preventivas sobre interrupciones de red y servicios.

Se debe revisar la configuración de Routers y Firewalls para detener las direcciones de Red inválidas, filtrar protocolos que no son necesarios e intensificar la inspección de tráfico.

El plan puede contemplar un enfoque híbrido, en el cual un dispositivo instalado "localmente" ("*on premise*"), reduce la frecuencia en la que la Entidad requiera realizar un proceso de cambio ("*switch-over*") hacia la Nube, minimizando costos asociados y asegurando una protección eficaz contra éste y otros tipos de ataques.

Bajo éste enfoque, se ofrece la mejor solución con capacidad de recuperación y escalabilidad de aplicaciones basadas en la Nube, y la visibilidad, protección e inspección granular en tiempo real del tráfico, bajo aplicaciones "on premise".

Justificación: Establecer una estrategia que integre todas las normas de este apartado "Gestión del Perímetro de Seguridad", para una efectiva defensa ante los ataques de denegación de servicios.

20.7 **Gestión de Eventos e Información de Seguridad (SIEM)**

Norma: Se recomienda la implementación de una Solución SIEM ("*Security Information Event Management*"), la cuales son plataformas que proporcionan análisis en tiempo real de los eventos de seguridad generados por los equipos de comunicación, servidores (seguridad, base de datos) y todo aquello que se esté monitoreando. Supervisa el tráfico, recolectan, analizan y priorizan los eventos de seguridad dentro de la red (bitácoras, amenazas, riesgos), y además se generan informes de cumplimiento.

Justificación: Contar con una solución que permita recopilar la mayor cantidad de información de las actividades realizadas y buscar rastro de actividad anormal en la infraestructura.

20.8 **Definición de zona de seguridad**

Norma: En la configuración de los Cortafuegos, se debe definir una zona comúnmente llamada "Zona Desmilitarizada" (DMZ), la cual se ubica entre la red interna (LAN – "Local Area Network") y la red externa (Internet). En la DMZ se ubican los servidores de correo electrónico, Web y el "Domain Name System" (DNS).

Justificación: Establecer los límites de seguridad necesarios para la protección de la red interna de la entidad.

20.9 **Acceso a servicios de correos externos (correos no institucionales)**

Norma: Se recomienda que el cortafuego esté configurado para bloquear el acceso de los funcionarios a servicios de correo externo, restringiendo los puertos de entrada y salida de la red, a servicios de correo externo (gmail, hotmail, yahoo, entre otros).

Justificación: Asegurar el uso del correo institucional para el manejo de la información de la Entidad.

21 Software Malicioso (Malware)

21.1 Prevención proactiva

Norma: El área responsable en la Unidad de TI debe establecer un control de verificación sobre la existencia de software malicioso en los equipos informáticos de la Entidad. Para ésta labor, se debe seleccionar herramientas especializadas contra este tipo de software. El personal encargado de seguridad informática será el responsable de administrar estas herramientas.

Justificación: Establecer un control para la prevención de daños a la información por causa del software malicioso.

21.2 Antivirus

Norma: Todos los servidores y computadoras deben tener instalados una solución de antivirus, a fin de garantizar el correcto funcionamiento e integridad de los sistemas informáticos.

Justificación: Mantener los sistemas de la Entidad protegidos y en funcionamiento.

21.3 Actualizaciones

Norma: La Unidad de TI es la responsable de mantener actualizados los programas de antivirus y malware, y verificar que el procedimiento de actualización diaria de firmas se esté realizando automáticamente y en forma correcta.

Justificación: Mantener las herramientas actualizadas contra nuevas amenazas de software malintencionado.

22 Tecnología Verde

22.1 Establecer Estrategia de Tecnología Verde o Ambiental

Norma: Se recomienda que la Unidad de TI implemente el concepto de "Tecnología Verde". Estas se refieren al uso eficiente de los recursos computacionales, minimizando el impacto ambiental, maximizando su viabilidad económica y asegurando deberes sociales. No sólo identifica a las principales tecnologías consumidoras de energía y productores de desperdicios ambientales, sino que ofrece el desarrollo de productos informáticos ecológicos y promueve el reciclaje computacional. Algunas de las tecnologías son clasificadas como verdes debido a que contribuyen a la reducción en el consumo de energía o emisión de dióxido de carbono son: computación en Nube, sistema de computación distribuido, virtualización en centros de datos, reducción del consumo de energía, entre otros.

Establecer la responsabilidad en lo referente al uso y su planificación sobre el diseño e implementación de las medidas en materia de las Tecnologías Verdes a la Unidad de TI.

Justificación: Reducción en uso de energía y cuidado ambiental.

22.2 Diagnóstico del nivel de implementación de las Estrategias

Norma: En el momento que la Unidad de TI, acuerde implementar Tecnología Verde en la Entidad, debe efectuar un diagnóstico para establecer el nivel en el que se encuentra la entidad con relación a las implementaciones de la tecnología verde, y los elementos a verificar son los siguientes:

- Iniciativas de tecnología verdes existentes.
- Metodologías de ahorro.
- Equipos electrónicos certificados bajo el programa "Energy Star".
- Metodología de reciclaje.

Justificación: Establecer las acciones y hoja de ruta para el uso de las Tecnología Verdes en la Entidad.

22.3 Actualización de las Estrategia

Norma: La estrategia de Tecnologías Verdes de la entidad, debe ser revisada y actualizada una vez al año.

Justificación: Mantener vigente estrategia de implementación acorde a la disponibilidad de nuevas Tecnologías Verdes en el mercado.

22.4 Desechos tecnológicos tóxicos y no tóxicos

Norma: El área responsable en la Unidad de TI, debe establecer un procedimiento para clasificar los desechos tecnológicos en tóxicos y no tóxicos, según las buenas prácticas sobre la materia, impulsando los procedimientos y medidas pertinentes para el manejo de los desechos tecnológicos.

Justificación: Buen cuidado ambiental.

22.5 **Manejo de las baterías de los equipos de Respaldo de Energía**

Norma: El área responsable en la Unidad de TI, debe coordinar con la administración de la entidad la recolección de las baterías gastadas o dañadas, con el fin de evitar ácidos o gases perjudiciales al medio ambiente y estas deben descartarse de forma adecuada.

Justificación: Manejo eficiente del descarte de las baterías y similares.

22.6 **Cumplimiento de la Norma Verde al momento de adquirir Impresoras**

Norma: Se recomienda que las impresoras adquiridas por la Entidad cumplan con las siguientes funcionalidades:

- Impresión a doble cara (se sugiere que sea la configuración por defecto).
- Control de impresiones por usuario.
- Generación de registro de impresiones por usuario o departamentos.
- Modo de hibernación cuando no esté en uso.

Justificación: Reducción en el consumo de papel y conservación de la energía.

23 Uso y manejo de la información

23.1 Clasificación de información

Norma: Para los efectos de aplicación e interpretación en materia de clasificación de información en las entidades, se debe utilizar como referencia, la Ley N° 6 de 22 enero de 2002, que "dicta normas para la transparencia en la gestión pública, establece la acción de Hábeas Data y dicta otras disposiciones", en su artículo N° 1 numeral 5, 6, 7, o vigente.

Información Confidencial: Todo tipo de información en manos de agentes del Estado o de cualquier entidad pública que tenga relevancia con respecto a los datos médicos y psicológicos de las personas, la vida íntima de los particulares, incluyendo sus asuntos familiares, actividades maritales u orientación sexual, su historial penal y policivo, su correspondencia y conversaciones telefónicas o aquellas mantenidas por cualquier otro medio audiovisual o electrónico, así como la información pertinente a los menores de edad. Para efectos de esta Ley, también se considera como confidencial la información contenida en los registros individuales o expedientes de personal o de Recursos Humanos de los funcionarios.

Información de acceso libre: Todo tipo de información en manos de agentes del Estado o de cualquier entidad pública que no tenga restricción.

Información de acceso restringido: Todo tipo de información en manos de agentes del Estado o de cualquier entidad, cuya divulgación haya sido circunscrita únicamente a los funcionarios que la deban conocer en razón de sus atribuciones, de acuerdo con la Ley

Recomendamos, que la información debe ser agrupada por los propietarios dentro de estos niveles de clasificación.

Justificación: Proporcionar una clasificación de la información para que los funcionarios públicos estén anuentes del tipo de información que manejan y fijen el grado de discreción y cuidado a utilizar.

23.2 Confidencialidad de la información

Norma: La información clasificada como confidencial o restringida, solo puede ser utilizada para propósitos de la función, servicio o actividad de la oficina pública y no debe ser divulgada a terceros.

Justificación: Proteger los datos con información confidencial.

23.3 Notificación de la pérdida o revelación de información sensible

Norma: Si existen indicios que información confidencial o restringida, ha sido revelada a personas no autorizadas o ha sufrido algún tipo de pérdida de la misma, el Jefe de la Unidad de TI, notificará al Director del área y al Despacho Superior de la entidad.

Justificación: Tomar las medidas correctivas para evitar la sustracción de información sensible y que esta sea utilizada en perjuicio del Estado o de los ciudadanos.

23.4 Retiro de información institucional, de las instalaciones públicas

Norma: El funcionario tiene terminantemente prohibido retirar de la Entidad: documentos, correspondencia, formularios, estadísticas o registros. Si por razones de sus funciones tiene

la necesidad de hacerlo, debe gestionar la autorización del Despacho Superior, Director o Jefe que le asignó la tarea.

Justificación: Resguardar la información que es propiedad del Estado.

23.5 **Cláusula de confidencialidad de los funcionarios**

Norma: Se recomienda establecer, un acuerdo de confidencialidad como parte de la inducción del funcionario y sus responsabilidades en la entidad, en donde se comprometa a no divulgar sin autorización, información que ponga en riesgo la confidencialidad de la Entidad o de los datos a su cargo.

Justificación: Proteger y cuidar la información sensitiva de la entidad.

24 Buen uso y protección de los equipos

24.1 Responsabilidad del funcionario en relación a su equipo asignado

Norma: Todo equipo tecnológico asignado al funcionario debe ser utilizado estrictamente en tareas relacionadas con su trabajo o función. Los dispositivos que la Entidad les proporcione a los funcionarios son para el uso exclusivo en acorde a las funciones asignadas, o aquellas que expresamente se les autorice, y no para uso personal. La Unidad de TI en conjunto con Bienes Patrimoniales establecerá los mecanismos de control para la asignación de los equipos así como la autorización para el uso de los equipos en actividades fuera de la Entidad.

Justificación: Buen uso y cuidado de los bienes del Estado.

24.2 Configuración del sistema operativo

Norma: Ningún funcionario está autorizado para modificar las propiedades o parámetros del sistema operativo y/o programas en los equipos asignados. De requerir algún cambio de esta naturaleza, el funcionario debe solicitarlo al personal de Soporte Técnico a través de la Mesa de Ayuda de la entidad. Precisar quién es el personal autorizado y la forma de gestionar cambios a los equipos propiedad de la entidad.

Justificación: Buen uso y cuidado de los bienes del Estado.

24.3 Apertura de equipos

Norma: Ningún funcionario está autorizado para abrir o desmontar equipos ante algún daño o problema que presente. De presentarse las situaciones antes mencionadas, el funcionario debe llamar a los operadores de la Mesa de Ayuda para que personal de Soporte Técnico solucione su problema.

Justificación: Cuidado de los bienes del Estado.

24.4 Instalación y desinstalación de programas informáticos

Norma: Se debe restringir a los funcionarios de la Entidad, la instalación o desinstalación de programas en los equipos de la Entidad. Para la instalación de un programa requerido por un funcionario por la naturaleza de sus actividades, éste debe solicitarlo a la Unidad de TI mediante el procedimiento establecido.

Justificación: Evitar implicaciones legales en derechos de propiedad intelectual que podría afrontar la entidad, además de los riesgos de seguridad que podrían presentarse.

24.5 Almacenamiento de archivos personales

Norma: Se restringe a los funcionarios o terceros el almacenamiento de archivos o información de carácter personal o ajeno a las funciones asignadas en los equipos de la Entidad.

Justificación: Prevenir la afectación por virus o software malicioso que puedan contener los archivos personales, en los sistemas de la Entidad.

24.6 Apagado de los Equipos Tecnológicos al final de la jornada laboral

Norma: Todo funcionario se encuentra en la obligación de apagar apropiadamente su equipo luego de finalizada su jornada laboral, salvo las excepciones que el personal de TI indique.

Justificación: Razones de seguridad y de ahorro de energía.

24.7 **Medios del almacenamiento externo**

Norma: Se recomienda que el funcionario no utilice medios de almacenamiento externos (memorias USB, etc.) o unidades lectoras de CD's/DVD's sin la debida autorización y, en caso de que cuenten con estos dispositivos, sean deshabilitados.

Justificación: Prevenir que los funcionarios instalen programas o que puedan grabar información confidencial de la Entidad en medios externos, así como prevenir la afectación por virus o software malicioso que puedan contener los archivos en los medios externos.

24.8 **Programas de uso en dispositivos particulares**

Norma: Todo funcionario que utilice cámaras o celulares inteligentes y requiera instalar programas relacionados a estos equipos en las computadoras de la Entidad, debe solicitar la aprobación de dicha instalación al director de su oficina, quien gestionara ante la Unidad de TI la instalación.

Justificación: Controlar el uso de los dispositivos particulares y programas relacionados que puedan afectar los sistemas de la Entidad.

25 Control de accesos, equipos y comportamiento

25.1 Controles en áreas restringidas

Norma: El área responsable en la Unidad de TI, debe implementar las medidas pertinentes, a fin de evitar el ingreso de personal no autorizado a las áreas restringidas de tecnología. Debe colocarse avisos de "Sólo Personal Autorizado", en las entradas y debe instalarse un Sistema de Control de Accesos que solo habilitará la entrada a los funcionarios por las responsabilidades de su cargo.

Justificación: Restringir el acceso a las áreas que contienen equipos que almacenen o procesen información sensitiva o crítica del Estado.

25.2 Mantener una lista del personal con acceso a áreas restringidas

Norma: Se debe mantener una lista actualizada de quienes tengan acceso a las áreas restringidas. Esta lista debe ser revisada y controlada periódicamente por la Unidad de TI de TI.

Justificación: Mantener el control y trazabilidad de acceso.

25.3 Fumar, comer o beber en áreas con equipos

Norma: Los funcionarios y visitantes tienen prohibido fumar, comer, beber, utilizar químicos en áreas cercanas a los servidores o sobre las computadoras e impresoras. Se recomienda la colocación de letreros para tal efecto.

Justificación: Reducir el riesgo de daños físicos a los equipos y a la información almacenada.

25.4 Uso de equipos personales en las redes institucionales

Norma: Se recomienda tomar las medidas para limitar la conexión a la Red Institucional con equipos personales, salvo que exista una autorización escrita por parte de la Unidad de TI.

Justificación: Evitar propagación de malware o el acceso desautorizado a los sistemas.

25.5 Retiro de equipos de las instalaciones públicas por parte de funcionarios

Norma: El retiro de equipo de las instalaciones no está permitido a los funcionarios, salvo aquellos que han sido expresamente autorizados por el jefe inmediato.

Justificación: Evitar la pérdida de información confidencial, aplicaciones, y activos lógicos y físicos propiedad de la entidad.

25.6 Tarjeta de acceso

Norma: Todo funcionario poseedor de una, tarjeta de acceso, tiene la responsabilidad de conservarla en buen estado. Estas no pueden ser transferidas o prestadas a otros funcionarios. De extraviarse, el funcionario está en la obligación de reportar inmediatamente al jefe de seguridad para que sea desactivada.

Justificación: Mantener el control de acceso a las facilidades.

26 Control de acceso a los sistemas y datos

26.1 Identificador del funcionario y contraseña

Norma: Todos los funcionarios deben tener una identificación única (usuario) y una contraseña, para el acceso a los sistemas, aplicaciones y a la red de la Entidad. Esta información es de carácter personal y confidencial y no debe ser compartida.

Justificación: Identificar y validar el acceso de los funcionarios a los sistemas por medio de credenciales de forma personal y restrictiva.

26.2 Longitud mínima de las contraseñas

Norma: Las contraseñas deben estar compuestas por un mínimo de ocho (8) caracteres alfanuméricos y caracteres especiales. La longitud mínima de la contraseña debe ser verificada automáticamente al momento de que el funcionario la ingrese al sistema. Esta norma puede ser reforzada con la prohibición de utilizar contraseñas utilizadas anteriormente y por el vencimiento automático de las contraseñas.

Justificación: Establecer una restricción de seguridad mínima.

26.3 Cambio periódicos de contraseña

Norma: El área responsable en la Unidad de TI debe implementar en sus sistemas, la obligatoriedad del cambio de contraseña a los funcionarios, preferiblemente en periodos mínimos de treinta (30) días.

Justificación: Protección de los sistemas y de la información.

26.4 Contraseñas temporales

Norma: Los sistemas deben ser configurados de tal forma, que al momento del ingreso del funcionario por primera vez al sistema, se valide la sesión inicial y fuerce al funcionario a introducir una nueva contraseña, la cual debe cumplir con los parámetros establecidos para la construcción de la misma.

Justificación: Garantizar que sólo el funcionario final conozca su contraseña.

26.5 Definición del vencimiento de contraseñas

Norma: Cuando la contraseña del funcionario esté próxima a expirar, recomendamos cinco (5) días antes, el sistema debe informar de este evento al usuario con la fecha de caducidad de su contraseña. Esta información debe ser desplegada en pantalla cuando el funcionario inicie sesión en su computador.

Todos los funcionarios deben tener presente que sus contraseñas son temporales y que por ello deben cambiarla cada cierto tiempo.

Justificación: Seguridad en el acceso a los sistemas.

26.6 Límite de intentos fallidos para acceder al sistema

Norma: El límite de intentos fallidos consecutivos, al realizar el proceso de acceder a los sistemas, debe ser definido estrictamente en no más de tres (3) intentos consecutivos; al tercer intento fallido el sistema debe inhabilitar, permanentemente o por lo menos diez (10) minutos, la cuenta del funcionario que intenta realizar la conexión.

El funcionario debe notificar al personal de la Mesa de Ayuda cuando la cuenta se inactive para que sea habilitarla nuevamente.

Justificación: Robustecer las medidas de seguridad en el proceso de acceder a los sistemas para evitar los accesos no autorizados.

26.7 **Contraseñas utilizadas más de una vez**

Norma: Se recomienda que en el proceso de cambio o renovación de las contraseñas, el sistema no permita al funcionario usar la misma contraseña que ha utilizado anteriormente. El sistema debe ser configurado para no permitir reutilizar ninguna de las últimas diez contraseñas.

Justificación: Minimizar el riesgo que las contraseñas puedan ser conocidas o deducidas.

26.8 **Anotar las contraseñas y dejarlas en lugares visibles**

Norma: Se recomienda que el funcionario evite anotar su contraseña y dejarla a la vista de otras personas.

Justificación: Minimizar la vulnerabilidad de acceso a los sistemas por personal no autorizado.

26.9 **Compartir contraseñas y nombres de usuarios**

Norma: Bajo ninguna circunstancia, los nombres de usuarios y las contraseñas deben ser compartidas o reveladas a otra persona. La responsabilidad de las acciones que un tercero pueda tomar por el uso de la cuenta de funcionario, recae en el funcionario dueño de la contraseña.

Justificación: Mantener la seguridad de los sistemas y trazabilidad en los accesos.

26.10 **Contraseñas distintas para cada proceso de autenticación**

Norma: Se recomienda, que el personal con asignaciones o roles especiales, se les debe asignar contraseñas para cada proceso de autenticación (red, aplicaciones críticas).

Justificación: Se busca evitar que un intruso o atacante interno o externo que tenga acceso a una contraseña, logre el acceso a todos los sistemas y servicios utilizados por ese funcionario.

26.11 **Bloqueo manual o automático del sistema**

Norma: En el caso que el funcionario necesite alejarse momentáneamente de su puesto de trabajo u oficina, el mismo debe bloquear manualmente su computador con el objetivo de no dejar su sesión abierta. Adicionalmente, el sistema debe contar con una política de tiempo en la cual el computador bloquee automáticamente la sesión.

Justificación: Prevenir la utilización indebida de un equipo que tenga el acceso activado.

26.12 **Salir de los sistemas al utilizar aplicaciones sensibles**

Norma: Si la aplicación a la cual los funcionarios se conectan se trata de pantallas que permitan modificar, adicionar o eliminar información sensible, el funcionario no debe salir de la aplicación sin antes cerrar la sesión del sistema.

Justificación: Prevenir el acceso, perdida o modificación de información.

26.13 **Resguardo de contraseñas**

Norma: Las contraseñas de Administración de todos los sistemas deberán guardarse individualmente en sobres cerrados y firmados en un lugar seguro y restringido. Esto debe realizarse periódicamente cada vez que requieran ser cambiadas por su vencimiento o actualizadas por cambios de personal o reasignación de roles.

Justificación: Asegurar la recuperación de acceso a la administración de los sistemas y mantener la seguridad en caso de pérdidas de contraseñas o cambio de roles.

26.14 **Doble autenticación**

Norma: Se recomienda que en el caso de ser requerido, por ejemplo en sistemas críticos de la Entidad que puedan accederse remotamente y lo ameriten, la Unidad de TI debe considerar la utilización de doble autenticación para aumentar el nivel de se seguridad de acceso a los mismos.

Justificación: Asegurar el acceso a los sistemas solamente por el personal permitido.

26.15 **Uso de CAPTCHA**

Norma: Se recomienda considerar la utilización de un CAPTCHA cuando se requiera asegurar el ingreso solamente por humanos, por ejemplo, en el uso de formularios de contacto o consultas por medio de la página Web de la Entidad, principalmente en plataformas con servicios de acceso público.

Justificación: Permitir el acceso a los sistemas solamente por personas.

27 Accesos y usos del Internet

27.1 Responsabilidad del funcionario en relación al uso de Internet

Norma: Todo funcionario con acceso a Internet, debe hacer uso de este servicio para actividades propias del trabajo.

Justificación: Uso adecuado de los bienes del Estado y del ancho de banda de Internet disponible.

27.2 Modificar la configuración de la estación de trabajo para navegar por Internet

Norma: Se recomienda implementar medidas de restricción a los funcionarios que le impidan modificar la configuración de sus equipos para navegar por Internet. Los cambios en equipos sólo podrán ser realizados por personal del área responsable en la Unidad de TI.

Justificación: Controlar la configuración del acceso a Internet.

27.3 Acceso a sitios Web prohibidos y material inadecuado

Norma: Se deben tomar las medidas para restringir el acceso a sitios Web de contenido adulto o pornográfico, apuestas, juegos de azar, juegos en línea, juegos interactivos y cualquier otro de contenido ajeno a sus funciones.

Justificación: Controlar el uso indebido del Internet, el cual debe ser de uso exclusivo para fines de trabajo y actividades de la Entidad.

27.4 Descarga y almacenamiento de material inadecuado

Norma: Se deben tomar las medidas para restringir la descarga de programas o material no relacionado con su trabajo o función en los equipos tecnológicos institucionales.

Justificación: Uso adecuado de los bienes del Estado y del ancho de banda de Internet disponible.

27.5 Sintonización de audio o vídeo a través del Internet

Norma: El Jefe de la Unidad de TI, deben tomar medidas para restringir el acceso a servicios online de música o televisión utilizando el Internet en temas no relacionados a la Entidad o a la responsabilidad del funcionario.

Justificación: Uso adecuado de los bienes del Estado y del ancho de banda de Internet disponible.

27.6 Llamadas telefónicas a través de Internet

Norma: El uso de la conexión de Internet, para realizar llamadas telefónicas estará permitido para casos previamente autorizados por el director o jefe del área responsable donde labora el funcionario, quien comunicará a la Unidad de TI de este requerimiento.

Justificación: Uso adecuado de los bienes del Estado y del ancho de banda de Internet disponible.

28 Servicio de correo electrónico institucional

28.1 Cuenta de correo electrónico del funcionario

Norma: Todo funcionario debe utilizar una cuenta del sistema de correo electrónico de la Entidad y no de dominios o servicios gratuitos o públicos como Gmail o Hotmail entre otros.

Justificación: Seguridad de la autenticidad de los correos institucionales y asignación de cuentas oficiales.

28.2 Uso del servicio de correo

Norma: Todo funcionario tiene el deber y la obligación de hacer un buen uso del servicio de correo institucional y utilizarlo sólo para asuntos relacionados con su trabajo. No debe utilizar este servicio para el envío de asuntos personales, publicidad, adjuntos de gran tamaño, correo basura o "spam" y cadenas, a otros funcionarios o destinatarios externos a la Entidad.

Justificación: Mantener la seguridad y la integridad del correo electrónico institucional.

28.3 Archivos adjuntos

Norma: Los archivos adjuntos en los mensajes del correo electrónico, deben estar estrictamente relacionados con el trabajo y se recomienda que el tamaño máximo permitido en los archivos adjuntos, no exceda 10 MB. Se prohíbe el envío de archivos de contenido ajeno a sus funciones.

El Jefe de la Unidad de TI puede autorizar el aumentar el tamaño de los archivos adjuntos a los funcionarios por la naturaleza de su cargo o función lo requieran.

Justificación: Mantener la integridad del correo electrónico institucional y racionalizar las capacidades de transmisión y almacenamiento de datos.

28.4 Compartir la cuenta de correo

Norma: Esta totalmente prohibido que los funcionarios públicos compartan el acceso de su cuenta de correo institucional.

Justificación: Resguardar la información del Estado.

29 Custodia de Datos por Terceros

29.1 Custodia de soportes digitales o servicios tercerizados de copias de seguridad

Norma: Se debe acreditar que el contrato por la prestación de los servicios señalados, contenga cláusulas que establezcan la correcta administración, manejo, devolución y/o destrucción de los datos y/o archivos al momento de finalizar el contrato.

Justificación: Evitar la manipulación no autorizada de los datos o archivos de la Entidad posterior a la finalización de la relación contractual.

29.2 Acuerdo de Confidencialidad sobre la información

Norma: Se debe asegurar que se establezcan clausulas dentro del contrato o se constituya un Acuerdo de Confidencialidad con las empresas prestadoras de servicios tercerizados, relacionados a la custodia y/o administración de datos o archivos.

Justificación: Establecer las obligaciones de la empresa, con respecto a mantener confidencial la información recibida.

30 Consideraciones de Servicios de Computación en la Nube (Cloud) y de Alojamiento (Hosting)

30.1 Adquisición de Servicios de Nube y de Alojamiento

Norma: Se debe realizar un análisis y un dimensionamiento apropiado antes de la adquisición y utilización de Servicios de Nube o de Servicios de Alojamiento. Dicho dimensionamiento debe estar enfocado en el tipo y tamaño de los recursos a adquirir, su Costo Total de Propiedad (TCO), en el tiempo, y previendo que se tienen, y tendrán, los presupuestos apropiados para cubrir con dichos servicios cuando sean o no requeridos.

Justificación: Resguardar la inversión del Estado en servicios externos a la Entidad.

30.2 Análisis de Riesgo de utilización de Servicios de Nube y de Alojamiento

Norma: Antes de contratar un servicio de Nube o alojamiento, el área responsable deberá realizar un análisis de los riesgos inherentes a la utilización de éstos para concluir la respectiva viabilidad de gestión, operativa, tratamiento y comunicación de la información.

Justificación: Asegurar una decisión correcta al momento de contratar servicios externos de computación.

30.3 Restricción de uso de plataformas críticas o de seguridad del Estado

Norma: No se deben utilizar servicios de Nube pública para plataformas de misión crítica o de seguridad del Estado sin la debida autorización del Jefe de la Unidad de TI de la Entidad y de la Autoridad de Innovación Gubernamental, así como también se debe considerar: la redundancia, seguridad, y los respaldos apropiados.

Justificación: Protección, disponibilidad y seguridad de la información, así como los servicios de la Entidad y del ciudadano.

30.4 Portabilidad de los Datos para los Servicios de Nube o de Alojamiento

Norma: Antes de contratar un servicio, el Jefe de la Unidad de TI de la Entidad deberá comprobar si el proveedor de servicios garantiza la portabilidad o migración de los datos y servicios (formatos de datos e interfaces de servicios estándar) en caso de cancelación del contrato, así como también deberá establecer de qué manera se va a hacer. Debe considerarse que los datos puedan ser recibidos apropiadamente y que puedan ser recuperados y restaurados para utilizarse. En cualquier caso, deberán acordarse cláusulas contractuales que estipulen formatos garantizados y la preservación de las relaciones lógicas.

Justificación: Garantizar la disponibilidad de los datos al terminar la relación contractual.

30.5 Confidencialidad de los Datos para los Servicios de Nube y de Alojamiento

Norma: La información en los servicios de Nube o alojamiento deben conservar su confidencialidad de acuerdo a la reglamentación y leyes vigentes en concepto de información digital del Estado y sus ciudadanos. Debe procurarse que solamente personal de la Entidad, o aquellas expresamente autorizadas, pueda tener acceso a cualquier información o dato contenido en estos servicios.

Justificación: Mantener la seguridad y privacidad de los datos del país y sus ciudadanos.

30.6 **Sensibilidad de los Datos para los Servicios de Nube y de Alojamiento**

Norma: Solo se pueden colocar datos de la Institución en una Nube pública o en un alojamiento privado externo, si los mismos no son de índole sensitiva.

Justificación: Mantener la privacidad de los datos del país y sus ciudadanos.

30.7 **Utilización de los Datos para los Servicios de Nube y de Alojamiento**

Norma: La información que va a manejarse con los servicios de Nube o alojamiento no puede ser utilizada para análisis por medio de sus características, atributos, cantidades, volúmenes, metada o ningún tipo de cualidad que los defina, para obtener métricas, estadísticas, rendimiento o decisiones de inteligencia para beneficio del proveedor o de terceros, solo que sea expresamente incluido en el contrato, para un fin que beneficie al estado.

Justificación: Mantener la privacidad de la cualidad de los datos del país y sus ciudadanos.

30.8 **Soberanía de los Datos**

Norma: La información que va a manejarse con los servicios de Nube pública o alojamiento privado externo, deberán mantenerse dentro del territorio Nacional, o en su defecto, en centros de datos o en la Nube Computacional Gubernamental de la AIG.

Justificación: Proteger el acceso a datos sensibles o críticos del país y de sus ciudadanos.

30.9 **Disponibilidad de los Servicios de Nube y de Alojamiento**

Norma: Se recomienda que los servicios de Nube o alojamiento estén, por lo menos, con una disponibilidad garantizada del 99.8%.

Justificación: Garantizar un alto nivel de disponibilidad acorde a los estándares mundiales.

30.10 **Versiones de los Servicios de Nube o de Alojamiento**

Norma: Se debe asegurar que se contemplen las actualizaciones de versiones necesarias para garantizar la continuidad de las características adquiridas, sin costos adicionales ni detrimento de éstas, a causa de nuevas o actualizadas opciones de los servicios contratados.

Justificación: Garantizar la continuidad de los servicios y que no sean afectados por nuevas o mejores características ofrecidas por los proveedores de dichos servicios.

30.11 **Devolución de la información y los datos al cancelar o terminar los Servicios de Nube o Alojamiento**

Norma: Una vez finalizada la relación contractual, la información deberá ser devuelta por la empresa contratada, al igual que cualquier soporte o documentos en que conste información alguna, y cualquier dato remanente en los servicios debe ser eliminado del centro de datos del proveedor.

Justificación: Resguardar la información del Estado y de sus ciudadanos.

30.12 **Contrato de prestación de los Servicios de Nube y de Alojamiento**

Norma: Se recomienda que el contrato de Servicios de Nube y de alojamiento incorpore entre sus cláusulas:

- Garantías respecto al no uso de los datos
- La seguridad
- Propiedad
- Controles de acceso y gestión de la información
- Propiedad intelectual de las aplicaciones
- Auditorías
- Tiempo de devolución de los datos
- Pautas que garanticen la correcta administración, devolución o destrucción de los datos al finalizar el contrato.

Justificación: Resguardar la información del Estado, estableciendo clausulas regulatorias en los contratos de servicios.

31 GLOSARIO

Considere las siguientes definiciones de uso, al presente documento.

1. **Activos de Información**: son elementos considerados de interés para los objetivos de la entidad. Son los recursos necesarios para que una institución funcione.
   - Datos
   - Software
   - Hardware y redes de comunicación
   - Sistemas y aplicaciones de informática
   - Servicios contratados
2. **Administrador de Seguridad Informática:** Gestiona la seguridad de los sistemas informáticos y de telecomunicaciones.
3. **Ancho de Banda:** cantidad de datos que pueden enviarse y recibirse en el marco de una comunicación. Suele usarse con referencia a la tasa de transferencia de datos, y se adquieran en rango suficiente para la demanda de la entidad.
4. **Antispam:** Método, servicio o software utilizado para prevenir los correos electrónicos no deseados (conocidos como SPAM). Es una protección para el servicio de correo electrónico con reglas que permiten reducir, la entrada tanto de spam, como de correo que contienen virus informáticos.
5. **Appliance:** Término para indicar la función de un dispositivo electrónico (hardware), diseñado para una aplicación o función específica. Equipado con un software integrado (firmware) con la función del sistema operativo y utilizado para llevar a cabo detalles complejos y funciones masivas de aplicaciones de software.
6. **Ataques de Denegación de Servicios (DoS):** "Denial of Service", es una agresión a un sistema de computadoras o red, que origina que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda (de la red de la víctima), o sobrecarga los recursos computacionales del sistema de la víctima.
7. El **DDoS** ("Distributed Denial of Service"), es una ampliación del ataque DoS, se genera un gran flujo de información desde varios puntos de conexión y es realizado por un conjunto o red de robots informáticos (o bots), que se funcionan de manera autónoma y automática. Bots es una técnica de ciberataque eficaz, sencilla y usual en este tipo de ataque.
8. **Bitácoras:** es un registro (archivos), de eventos durante un periodo de tiempo, donde el administrador del sistema recurre en busca de información y/o registros de actividad, con el objeto de determinar la causa de un problema, o bien como una actividad de control.
9. **Cableado Estructurado:** Sistema de cables, conectores, y dispositivos que permiten establecer una infraestructura de telecomunicaciones informáticas en un edificio.
10. **Configuración:** conjunto de datos que determina el valor de algunas variables de un programa, dispositivo o de un sistema operativo.
11. **Corta Fuego**: El cortafuegos o "firewall" es un dispositivo diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos.
12. **Corta Fuego de Aplicación WEB (WAF):** Un Cortafuego de aplicaciones Web o WAF ("Web Application Firewall"), es un servidor de seguridad que vigila, filtra o bloquea el tráfico HTTP hacia y desde una aplicación Web. Funciona como "appliance", servidor plug-in o servicio basado en la nube. Un WAF inspecciona todos los paquetes de datos HTML,

HTTPS, SOAP y XML-RPC. Previene ataques como XSS, inyección SQL, el secuestro de sesión y desbordamientos de búfer, que los cortafuegos de red y sistemas de detección de intrusos a menudo no son capaces de prevenir o manejar. Un WAF también es capaz de detectar y prevenir ataques desconocidos mirando los patrones nuevos y extraños en el tráfico de datos.

13. **Cloud:** Del inglés "Cloud Computing", y conocida también como: servicios en la Nube, Informática en la Nube, Nube Computacional, es un esquema que permite ofrecer servicios de computación a demanda en servidores virtuales a través de una red, que usualmente es Internet. El concepto fundamental es ofrecer un servicio de entrega de los recursos informáticos de computación o almacenaje requeridos a través de una red global: el Internet. El concepto de "nube informática" es muy amplio, y abarca casi todos los posibles tipos de servicio en línea, pero cuando las empresas ofrecen un producto alojado en la Nube, por lo general se refieren a alguna de estas tres modalidades: el Software como Servicio (**SaaS**), Plataforma como Servicio (**PaaS**) e Infraestructura como Servicio (**IaaS**).
14. **Custodio de activo de información:** Identifica a un funcionario, un cargo o proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.
15. **Dominio:** Representa una forma de organizar los equipos en las redes. Algunos de los equipos son servidores. Los administradores de red utilizan los servidores para controlar la seguridad y los permisos de todos los equipos del dominio, así resulta más sencillo efectuar cambios, ya que éstos se aplican automáticamente a todos los equipos dentro del dominio.
16. **En línea:** El concepto se utiliza en el ámbito de la informática para nombrar a algo que está conectado o a alguien que está haciendo uso de una red, generalmente, Internet.
17. **Encriptación:** codificación de la información (archivos, correo electrónico), para protegerla frente a terceros, mientras la información viaja por la red.
18. **Entidad:** Toda colectividad que puede considerarse como una unidad, en especial, cualquier corporación, compañía e entidad, etc.
19. **Equipo Servidor:** Es un equipo informático que forma parte de una red y provee servicios a otros equipos clientes.
20. **Filtrado de Contenido Web (Web Filter):** Un appliance o software que supervisa todo el tráfico HTTP entrante en la red y monitorear el comportamiento de los usuarios, bloqueado el contenido de la Web especificado o catalogado como "inapropiado". Se aplica en entornos que requieren un mayor nivel de protección o están sujetos a regulaciones.
21. **Unidad de TI:** la Gerencia, Dirección, Departamento u Oficina de TI es la dependencia en la Entidad, responsable de la gestión de las plataformas relacionadas a las tecnologías de la información y comunicación.
22. **Jefe de la Unidad de TI:** Gerente, Director, Jefe o persona a cargo de la Unidad de TI en la Entidad.
23. **Unidad Ejecutora de Gobierno Digital:** unidad de carácter interdisciplinario al más alto nivel de la Entidad responsable de liderar y dar seguimiento a las acciones institucionales establecidas en la Agenda Digital institucional, Plan de Simplificación de Trámites y el Plan Operativo Anual.
24. **Hardware:** Conjunto de elementos físicos que constituyen una computadora o un sistema informático.
25. **Interoperabilidad**: como la habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada.

26. **Máxima Autoridad de la Entidad**: Es la dependencia administrativa de más alta posición, en la jerarquía de la estructura organizacional de la entidad.
27. **Norma**: Regla que se debe seguir o a la que se deben ajustar las conductas, tareas, actividades, etc.
28. **On Premise**: Se refiere a la ubicación de la infraestructura de TI. Cuando se instala y se ejecutan los equipos localmente, en lugar de una instalación remota, o ante la opción de utilizar servicios en la nube.
29. **Periférico:** Dispositivo electrónico que se conecta o acopla a una computadora, pero no forma parte del núcleo básico (CPU, memoria, placa madre, alimentación eléctrica) de la misma.
30. **Propietario de activo de información:** Identifica a un funcionario, un cargo o proceso o grupo de trabajo designado por la entidad, y que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento el uso y la seguridad de los activos de información asignados.
31. **Servicios de TI:** Conjunto de actividades que buscan responder a las necesidades de un cliente por medio de un cambio de condición en los bienes informáticos (llámese activos), potenciando el valor de éstos y reduciendo el riesgo. Soporte a usuarios, aplicaciones, mesa de ayuda, otros.
32. **Infraestructura como Servicio (IaaS) (administración por el usuario):** En el caso de IaaS, los recursos informáticos ofrecidos consisten, en particular, en hardware virtualizados (servidores), en otras palabras, infraestructura de procesamiento, incluye aspectos como el espacio para almacenamiento, conexiones de red, ancho de banda, equipos de seguridad y balanceadores de carga. Físicamente, un catálogo de recursos de hardware disponibles procedes de un grupo de servidores, generalmente distribuidos entre numerosos centros de datos.
33. **Plataforma como Servicio (PaaS) (infraestructura y administración):** El concepto de PaaS, proporciona *una plataforma y un entorno* que permiten a los desarrolladores crear aplicaciones y servicios que funcionan a través de internet, y en donde los usuarios acceden a ellos a través de su navegador web. Herramientas de desarrollo, administración de Bases de Datos, además de todos los recursos ofrecidos bajo el esquema de IaaS, es lo que ofrece el proveedor. La infraestructura y las aplicaciones *se gestionan en nombre del cliente*, y se ofrece también soporte técnico.
34. **Software como Servicio (SaaS):** El concepto SaaS, se describe como cualquier servicio cloud en el que los consumidores acceden a las aplicaciones de software alojadas "en la nube" a través de cualquier dispositivo que pueda conectarse a internet. El modelo SaaS se conoce también como "software a demanda", por la forma de utilizarlos que se parece más a un alquiler de software por periodos determinados. El software ofimático es el mejor ejemplo posible de aplicación del modo SaaS.
35. **Servicios en línea:** Son servicios que se ofrece a través de Internet. Estos permiten consultar y hacer trámites utilizando un medio de rápido y de fácil acceso como es Internet.
36. **Servidor:** modelo de computadora de alta capacidad de procesamiento y almacenamiento, diseñada para alojar un conjunto de aplicaciones que tiene gran demanda dentro de una red.
37. **SIEM**: (Security Information and Event Management): Son plataformas que proveen análisis en tiempo real de los eventos de seguridad generados por los equipos de comunicación, servidores y todo lo que se esté monitoreando. El término proviene, de la combinación de SIM (Security Incident Management), y está en el segmento de la Administración de la

Seguridad y su campo abarca la Correlación de Eventos, Análisis en Tiempo Real, Flujo de Trabajo, además toma en consideración otras fuentes como el monitoreo del tráfico y el SEM (Security Event Management). Tiene que ver con el almacenamiento a largo plazo de logs para su posterior análisis y reporte. Esta combinación nos da en una sola plataforma con una serie de funcionalidades.

38. **Sistema de Detección de Intrusos (IDS):** Intrusion Detection System es una estructura para la detección de accesos no autorizados a un computador o a una red, que puede ser un software o appliances. El IDS suele tener sensores virtuales (por ejemplo, un sniffer ((analizador de protocolos) de red) con los que el núcleo del IDS puede obtener datos externos, generalmente sobre el tráfico de red. El IDS detecta, gracias a dichos sensores, las anomalías que pueden ser indicio de la presencia de ataques y falsas alarmas.
39. **Sistema de prevención de intrusos (IPS):** Intrusion Prevention System es un mecanismo proactivo de prevención de intrusos que puede ser un software o appliances que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos. Los IPS categorizan la forma en que detectan el tráfico malicioso:
    - Detección basada en firmas: como lo hace un antivirus.
    - Detección basada en políticas: el IPS requiere que se declaren muy específicamente las políticas de seguridad.
    - Detección basada en anomalías: en función con el patrón de comportamiento normal de tráfico.
40. **Sistema Operativo:** Conjunto de órdenes y programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas.
41. **Software:** Conjunto de programas y rutinas que permiten a los dispositivos realizar determinadas tareas.
42. **Switchover:** es el cambio manual o automático, de un sistema a un servidor redundante o que se encuentra en espera (standby) o red (física o nube) en caso de ausencia o de la terminación anormal del servidor, sistema o red, anteriormente activo.
43. **Tecnología de la Información y la Comunicación (TIC)**: Conjunto de tecnologías y aplicaciones para proveer a las personas y entidades de la información, su conectividad e interoperabilidad.
44. **Tramite en Línea**: Es un trámite realizado mediante el uso de las TIC en relación a un documento o expediente, sin estar presente físicamente en la entidad e incluye toda aquella acción que un usuario realice para dar respuesta al trámite.