República de Panamá

AUTORIDAD NACIONAL PARA LA INNOVACION GUBERNAMENTAL

Resolución No. 07
de 30 abril de 2025

"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, VERSIÓN 2.1"**

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 el cumplimiento de los mismos, disposición reglamentada mediante el Artículo 3 del Decreto Ejecutivo No. 205 de 9 de marzo de 2010, disponiéndose que, para el ejercicio de estas funciones, la AIG emitirá criterios e impartirá instrucciones mediante circulares y resoluciones a las entidades gubernamentales.

Que, en ejercicio de las facultades atribuidas, mediante la Resolución No. 3 de 22 de enero de 2024, la Autoridad Nacional para la Innovación Gubernamental aprobó el documento titulado "**NORMAS GENERALES PARA LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC) EN EL ESTADO en su versión 2.0"**, con el objetivo de mejorar y normalizar los procesos tecnológicos del Estado.

Que no obstante, ante la creciente importancia del concepto de **Soberanía de Datos,** incluido en las referidas normas, mediante la Resolución No. 3 de 22 de enero de 2024, la Autoridad Nacional para la Innovación Gubernamental, previa revisión del concepto vigente a esa fecha, procedió a actualizar la normativa para garantizar la protección de la información sensible del Estado Panameño, modificando la Norma 30.8 **"SOBERANIA DE LOS DATOS",** incluyéndose instrucciones de obligatorio cumplimento por parte de las entidades del Estado, haciéndose necesaria la incorporación a dichas Normas, de la definición actualizada, como parte de la versión 2.1., procediéndose a la publicación en la Gaceta Oficial.

Que, adicionalmente, la entidad ha considerado necesario, agregar a las normas aludidas lo referente a los "Modelos utilizados en el desarrollo de aplicaciones", para introducir que las entidades apliquen

Que el artículo 7 de la Ley 65 de 2009, establece que es función del Administrador General de la Autoridad Nacional para la Innovación Gubernamental, dirigir y administrar la entidad, por lo que en ejercicio de las facultades que le otorga la Ley,

RESUELVE:

PRIMERO: Aprobar el documento titulado: **"NORMAS GENERALES PARA LA GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (TIC) EN EL ESTADO, versión 2.1"**, tal cual se adjunta a la presente Resolución, de obligatorio cumplimento por parte de las entidades gubernamentales.

SEGUNDO: La Autoridad Nacional para la Innovación Gubernamental (AIG) por conducto de la Dirección de Cumplimiento, Normas y Soluciones Verticales, dará seguimiento, coordinación y control de las "Normas Generales para la Gestión de las Tecnologías de la Información y Comunicaciones (TIC), en el Estado, versión 2.1", para lo cual elaborará informes y publicará el "Ranking de Cumplimiento" por parte de las entidades gubernamentales.

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

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,

ADOLFO FABREGA
Administrador General

AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL
REPÚBLICA DE PANAMÁ

AIG
ASESORÍA
LEGAL

GOBIERNO NACIONAL
★ CON PASO FIRME ★

AIG
AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL

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

AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL (AIG)

Dirección de Cumplimiento, Normas y Soluciones Verticales

Abril 2025

SECRETARÍA GENERAL AIG

ADOLFO FÁBREGA
Administrador General

FRANCISCO GUINARD
Sub-Administrador General

ALFREDO REMON
Director de Cumplimiento, Normas y Soluciones Verticales

JULIO A. PRESTAN
Dirección de Cumplimiento, Normas y Soluciones Verticales

PATRICIO KU
Dirección de Cumplimiento, Normas y Soluciones Verticales

JOEL LUQUE
Dirección de Cumplimiento, Normas y Soluciones Verticales

Fecha	23/04/2025
Versión	2.1
Nivel de difusión	Público
Estatus	Documento Final
Documento aprobado por	Adolfo Fabrega

ÍNDICE

1. Introducción 11
2. Sujetos de la Norma 12
3. Marco Legal 13
4. Cumplimiento de los lineamientos indicados en la Ley N°83, su reglamentación y otras disposiciones. 14
   - 4.1 Trámites en Línea 14
   - 4.2 Formularios para la gestión de los Trámites Digitales 14
   - 4.3 Plan de Simplificación de Trámites 14
   - 4.4 Aceptación de documentos firmados electrónicamente por los usuarios 14
   - 4.5 Excepción de los usuarios de aportar datos y/o documentos, cuando dicha información se encuentre en las bases de datos de las Entidades 14
   - 4.6 Habilitación de diferentes canales o medios para la prestación de trámites 14
   - 4.7 Uso de la Pasarela y Portal Nacional de Pagos 15
   - 4.8 Acceso sencillo y eficaz de la información pública 15
   - 4.9 Publicaciones Electrónicas 15
   - 4.10 Facilidad para las Personas con Discapacidad (PCD) o Personas en Situación de Discapacidad. 15
   - 4.11 Facilitar el acceso e intercambio de información entre Entidades Públicas. 15
   - 4.12 Cumplimiento de normas, estándares y condiciones en los sistemas tecnológicos 15
   - 4.13 Plan de Sistemas 15
   - 4.14 Agenda Digital Institucional 16
   - 4.15 Plan Operativo Anual 16
5. Normas de Aplicación General 17
   - 5.1 Unidad Ejecutora de Gobierno Digital 17
   - 5.2 Gestión de la Calidad en los Servicios 17
   - 5.3 Gestión de la Seguridad de la Información 17
   - 5.4 Gestión de Incidencias de Seguridad Informática 18
   - 5.5 Seguimiento a los Contratos de Tecnología 18
   - 5.6 Gestión de Proyectos de TI 19
   - 5.7 Regulaciones que afectan la Gestión de TI 19

SECRETARÍA GENERAL AIG

5.8 Inventario general de TI 19

6. De la Unidad de TI 20

6.1 Cargos o Puestos en las Dependencias de Tecnología de la Información 20

6.2 Segregación de funciones 20

6.3 Registro del personal de la Unidad de TI 20

6.4 Comunicación y explicación de las Normas Generales de TIC 20

6.5 Capacitación en Tecnología de la Información 20

6.6 Normas Internas de uso de las TIC 21

6.7 Establecimiento de métricas 21

6.8 Revisión de cumplimiento 21

7. Procedimientos en TI 22

7.1 Elaboración y prueba de los procedimientos de TI 22

7.2 Documentación de los procedimientos de TI 22

7.3 Aprobación de los Procedimientos, Políticas, otros de TI 22

7.4 Revisión y actualización de los procedimientos de TI 22

8. Administración Integral del Riesgo 23

8.1 Administración del riesgo tecnológico. 23

8.2 Evaluación del riesgo tecnológico 23

8.3 Tratamiento del riesgo 23

8.4 Seguimiento y revisión 24

8.5 Registro e Informe 24

9. Autorizaciones 25

9.1 Solicitud de Servicios a la Unidad de TI 25

9.2 Inspección de archivos en dispositivos institucionales 25

9.3 Traslado de dispositivos TIC 25

9.4 Privilegios o Controles de acceso a los datos 25

9.5 Privilegios y derechos de usuarios en servidores y sistemas institucionales 25

10. Gestión de Licencias de Software 27

10.1 Adquisición de programas informáticos 27

10.2 Evidencia de adquisición de los programas informáticos 27

10.3 Inventario de las licencias de los programas informáticos 27

10.4 Derechos de Propiedad Intelectual de las aplicaciones del Estado 28

10.5 Instalación y desinstalación de programas informáticos 28

SECRETARÍA GENERAL AIG

10.6 Comprobación de los programas informáticos 29
10.7 Renovación y/o Actualización de los programas informáticos y aplicaciones 29
11. Adquisición y mantenimiento de la infraestructura tecnológica 30
11.1 Evaluación, recomendación y controles para la adquisición de infraestructura tecnológica 30
11.2 Guías y Estándares Tecnológicos 30
11.3 Actualización de hardware 30
11.4 Cableado Estructurado y redes Inalámbricas 30
11.5 Contratación de terceros para la implementación y el mantenimiento 31
11.6 Tercerización de Administración y Gestión de Servidores 31
12. Administración de la infraestructura de servidores 33
12.1 Control de acceso a la sala de servidores 33
12.2 Privilegios en los servidores 33
12.3 Administración proactiva 33
12.4 Ubicación y condiciones de las salas de servidores 33
12.5 Protección de los servidores contra condiciones eléctricas 34
12.6 Bloqueo automático y doble autenticación en servidores 34
12.7 Recursos compartidos en servidores 34
12.8 Actualizaciones 35
13. Aplicaciones 36
13.1 Convenciones para el desarrollo de sistemas (software) 36
13.2 Incorporación de seguridad, al ciclo de vida del desarrollo de aplicaciones 36
13.3 Control de versiones en los Desarrollos de las Aplicaciones 37
13.4 Dependencia de la seguridad de otros sistemas de información 37
13.5 Avisos de fallas en las aplicaciones desarrolladas y su operación 37
13.6 Calidad de las aplicaciones 37
13.7 Pruebas a las aplicaciones 38
13.8 Ambientes separados para desarrollo, pruebas y producción 38
13.9 Documentación de la operación y entrenamiento de la aplicación 38
13.10 Sobre los Modelos utilizados en el desarrollo de aplicaciones 39
14. Base de Datos 40
14.1 Responsabilidades, roles y perfiles del área de soporte a la Base de Datos 40
14.2 Documentos físicos y digitales de la Base de Datos 42
14.3 Documentación técnica de la Base de Datos (diccionarios) 42

SECRETARÍA GENERAL AIG

14.4 Gestión de cambios en Base de datos 42
14.5 Realización de respaldos diarios a la Base de datos 43
14.6 Planificación de los procesos de depuración de datos y administración de espacio en disco 43
14.7 Gestión de la seguridad, integridad, accesos a aplicaciones y control de usuarios en Bases de Datos 43
14.8 Procesos de monitoreo 44
14.9 Configuración y mantenimiento de base de datos 44
14.10 Migraciones y replicación de datos y base de datos (internas/externas) 45
15. Monitoreo de las bitácoras 46
15.1 Eventos del Sistema 46
15.2 Bitácoras para el manejo de información confidencial 46
15.3 Período de retención de las bitácoras del sistema 46
15.4 Personal autorizado para la revisión de las bitácoras del sistema 46
15.5 Desarrollo de Rutinas de Bitácora 47
15.6 Revisión regular de las bitácoras del sistema 47
16. Administración de cambios en el ambiente de producción 48
16.1 La administración de cambios debe ser parte de un procedimiento formal 48
16.2 Evaluación de solicitudes de cambios en producción 48
16.3 Comunicación de cambios en la Tecnología de Información 48
16.4 Autorización de cambios directos a los datos en producción 49
16.5 Instalación de actualizaciones 49
16.6 Seguimiento a los cambios post-producción 49
16.7 Bitácora de cambios y actualizaciones 50
16.8 Documentación de las modificaciones realizadas a la aplicación 50
16.9 Acceso del personal de desarrollo al ambiente en producción 50
16.10 Identificación de errores o problemas en los sistemas o aplicaciones 50
17. Niveles del Servicio Técnico y relaciones con terceros 51
17.1 Primer nivel de servicio 51
17.2 Segundo nivel de servicio 51
17.3 Tercer nivel de servicio a los 51
17.4 Cláusula de confidencialidad 51
17.5 Administración de los bienes del Estado, utilizados por terceros 51
17.6 Devolución de los bienes del Estado al término de un Contrato 52
17.7 Conexión a la red local de la Entidad, con equipos tecnológicos de terceros 52

SECRETARÍA GENERAL AIG

17.8 Utilización de Internet de la Entidad, por parte de proveedores o visitantes 52
18. Continuidad del servicio....53
18.1 Gestión de la Continuidad de los Servicios de TI 53
18.2 Preparación y mantenimiento de un Plan de Contingencia 53
18.3 Implementación de un Plan de Recuperación de Desastres 53
18.4 Respaldo de Información 54
18.5 Proyectos de misión crítica, redundancia y alta disponibilidad 54
18.6 Topología de red y Diagramas de interconexión 54
19. Custodia de Datos por Terceros....55
19.1 Custodia de soportes digitales o servicios tercerizados de copias de seguridad 55
19.2 Principios Generales para la Custodia de datos por Terceros 55
19.3 Acuerdo de Confidencialidad sobre la información 55
19.4 Revisión anual de los procedimientos para la custodia de datos por Terceros 55
19.5 Registro de acceso y auditoría para la custodia de datos por terceros 55
19.6 Recuperación de información custodiada por terceros 55
19.7 Procedimientos para la eliminación de datos custodiados por terceros 56
20. Uso y manejo de la información 57
20.1 La Información como Activo 57
20.2 Clasificación de información 57
20.3 Confidencialidad de la información 57
20.4 Retiro de información institucional de las instalaciones públicas 58
20.5 Acuerdo de confidencialidad de los funcionarios de tecnología 58
21. Confidencialidad....59
21.1 Compromiso del Estado en la custodia de datos 59
21.2 Compromiso del funcionario con la seguridad de la información 59
21.3 Cifrado 59
21.4 Autorización para verificar los correos electrónicos en la Entidad 59
21.5 Análisis y monitoreo de la actividad en la red Institucional e internet de la Entidad 59
22. Gestión del perímetro de seguridad 60
22.1 Cortafuegos (Firewalls) 60
22.2 Sistema de Detección y Respuestas Gestionada a Amenazas (MDR) 60
22.3 Sistemas de Prevención y Detección de Accesos (IPS/IDS) 61
22.4 Protección del Correo Electrónico (Antispam) 61

SECRETARÍA GENERAL AIG

22.5 Protección contra Ataques de Denegación de Servicio (DoS - Denial of Service DDoS - Distributed Denial of Service)....62
22.6 Gestión de Eventos e Información de Seguridad (SIEM)....62
22.7 Gestión de zona de seguridad....62
22.8 Protección de Puntos de los Accesos Inalámbricos o Wi-Fi....63
22.9 Protección a la tecnología de Voz sobre IP (VoIP)....63
22.10 La Seguridad en las Operaciones y Comunicaciones....64
23. Software o Malicioso (Malware)....65
23.1 Prevención proactiva....65
23.2 Antivirus....65
23.3 Actualizaciones....65
24. Buen uso y protección de los equipos de cómputo....66
24.1 Responsabilidad del funcionario con relación a su equipo asignado....66
24.2 Configuración del sistema operativo....66
24.3 Desmontado de equipos....66
24.4 Almacenamiento de archivos personales....66
24.5 Apagado de los Equipos Tecnológicos al final de la jornada laboral....67
24.6 Medios del almacenamiento externo....67
24.7 Programas de uso en dispositivos particulares....67
25. Control de accesos....68
25.1 Control de acceso de equipos personales en las redes institucionales....68
25.2 Supervisión y control de sesiones de accesos remotos....68
25.3 Controles de accesos y seguridad física en áreas restringidas....68
25.4 Tarjeta de acceso....68
25.5 El Control de Acceso a los Sistemas....68
25.6 Accesos a los Sistemas de Información....69
25.7 Cambio periódico de contraseña....69
25.8 Contraseñas temporales....69
25.9 Notificación del vencimiento de contraseñas....70
25.10 Límite de intentos fallidos para acceder al sistema....70
25.11 Contraseñas distintas para cada proceso de autenticación....70
25.12 Bloqueo manual o automático del sistema....70
25.13 Doble autenticación....70

SECRETARÍA GENERAL AIG

25.14 Uso de CAPTCHA....71
26. Cambios en el control de acceso, por acciones de personal....72
26.1 Cambio en el control de acceso por Traslados o Reasignación del funcionario....72
26.2 Retiro de funcionarios....72
26.3 Vacaciones de funcionarios....73
26.4 Devolución de equipos del Estado....73
27. Accesos y usos del Internet....74
27.1 Responsabilidad de la entidad en cuanto al servicio de Internet....74
27.2 Responsabilidad del funcionario con relación al uso de Internet....74
27.3 Modificar la configuración de la estación de trabajo para navegar por Internet....74
27.4 Acceso a sitios Web prohibidos y material inadecuado....74
27.5 Descarga y almacenamiento de material inadecuado....74
27.6 Sintonización de audio o vídeo a través del Internet....74
27.7 Llamadas a través de Internet....75
28. Servicio de correo electrónico institucional....76
28.1 Uso de plataformas libres para correos electrónicos....76
28.2 Procedimiento de solicitud de correo electrónico....76
28.3 Cuenta de correo electrónico del funcionario....76
28.4 Responsabilidad del usuario en el servicio de correo....76
28.5 Pie de página de correo electrónico....76
28.6 Uso del servicio de correo....77
28.7 Archivos adjuntos....77
28.8 Utilizar la cuenta de correo en redes sociales....77
28.9 Compartir el acceso del correo....77
28.10 Deshabilitar cuentas de Correo Electrónico....77
28.11 Uso de correo eléctrico en dispositivos móviles personales....78
29. Tecnología Verde....79
29.1 Establecer estrategias de tecnología verde o ambiental....79
29.2 Diagnóstico del nivel de implementación de las estrategias....79
29.3 Actualización de la estrategia....79
29.4 Desechos tecnológicos tóxicos y no tóxicos....79
29.5 Manejo de las baterías de los equipos de respaldo de energía....80
29.6 Cumplimiento de la norma verde al momento de adquirir Impresoras....80

SECRETARÍA GENERAL AIG

29.7 Uso eficiente de impresoras 80
29.8 Implementación de un espacio físico por parte de la Unidad TI 80
29.9 Procedimientos de destrucción de datos y hardware 80
30. Consideraciones de servicios de computación en la nube (Cloud) y de alojamiento (Hosting) 82
30.1 Requisitos para adquisición de servicios en la nube y de alojamiento con terceros 82
30.2 Contrato de prestación de los servicios de nube o de alojamiento 82
30.3 Portabilidad de los datos para los servicios de nube o de alojamiento 82
30.4 Restricción de uso para servicios críticos o de seguridad del Estado 82
30.5 Confidencialidad de los datos para los servicios de nube y de alojamiento 83
30.6 Disponibilidad de los servicios de nube o de alojamiento 83
30.7 Versiones del hardware y software que conforman los servicios de nube o de alojamiento 83
30.8 Soberanía de Datos 84
30.9 Sensibilidad de los datos en servicios en la nube 85
30.10 Establecimiento de controles para servicios en la nube 85
30.11 Alta disponibilidad de los servicios en la nube institucional 85
31. Teletrabajo 86
31.1 Unidad responsable del Teletrabajo 86
31.2 Recursos informáticos para el Teletrabajo 86
31.3 Controles en el Teletrabajo 86
31.4 Seguridad en el Teletrabajo 86
31.5 Soporte en el Teletrabajo 87
32. GLOSARIO 87

SECRETARÍA GENERAL AIG

1. Introducción

La Autoridad Nacional para la Innovación Gubernamental (AIG), ha constituido las presentes Normas Generales para la Gestión de las Tecnologías de Información y Comunicación (TIC), con el objetivo principal de normalizar los procesos operativos y aplicar buenas prácticas de administración y uso de las tecnologías, lo que contribuye al fortalecimiento de las Plataformas e Infraestructuras Tecnológicas en las entidades del Estado.

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

Los lineamientos de control, como las recomendaciones o sugerencias deben ser acatados en la gestión y uso de los recursos de TIC en el Estado, prácticas que facilitarán las tareas de verificación e inspección del cumplimiento de lo indicado.

Esta es la versión 2.1 de las Normas y la AIG procederá a su actualización, según se produzcan cambios en los procedimientos y las tecnologías.

2. Sujetos de la Norma

Esta normativa es aplicable al Órgano Legislativo, Órgano Judicial, Órgano Ejecutivo (Gobierno Central, Entidades Autónomas y Semiautónomas, Empresas Públicas, los Intermediarios Financieros del Estado), Patronatos regentes de Entidades o Bienes Públicos, el Régimen Municipal (en las áreas que aplique según el ente que administra el tema de tecnología), sociedades anónimas en las que el Estado es propietario del cincuenta y uno por ciento (51%) o más de sus acciones del patrimonio de la República de Panamá.

Se exceptúan de la observancia de estas normativas, aquellos casos en que las leyes especiales disponga otro régimen.

Es deber de todo Gerente, Director o Jefe de la Unidad de Tecnología de la Información (TI), en las instituciones el cumplimiento de las Normas y su difusión.

3. Marco Legal

Ley N°65 del 30 de octubre de 2009, 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 esta materia".

El marco legal que fundamenta a esta Norma, lo componen, además de la Ley N°65, las leyes y decretos ejecutivos emitidos y sus modificaciones que complementan la referida Ley.

SECRETARÍA GENERAL AIG

4. Cumplimiento de los lineamientos indicados en la Ley N°83, su reglamentación y otras disposiciones.

4.1 Trámites en Línea

Norma: La Entidad debe brindar, en la medida de sus posibilidades la opción de gestión de sus trámites en línea". Los tramites deben ser incluidos en el Portal Oficial "Panamá Digital", con la información de los requisitos que deben cumplir para su tramitación.

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 este nivel, deberá publicitar la información en los medios de comunicación y en el Portal Oficial para trámites del estado.

4.2 Formularios para la gestión de los Trámites Digitales

Norma: Cuando el trámite incluye el uso de formularios, la Entidad debe proveerlos de forma digital y en formato de datos abiertos en su Portal Oficial.

4.3 Plan de Simplificación de Trámites

Norma: La Entidad elaborará anualmente un Plan para la Simplificación de sus procesos administrativos y los trámites que guarden relación con los ciudadanos.

4.4 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 ológrafa.

4.5 Excepción de los usuarios de aportar datos y/o documentos, cuando dicha información se encuentre en las bases de datos de las Entidades

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 de interoperabilidad y 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.

4.6 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.

En la medida de sus posibilidades, debe ofrecer versiones en otros idiomas en sus páginas Web, de acuerdo con el alcance de operación de la Entidad.

4.7 Uso de la Pasarela y Portal Nacional de Pagos

Norma: La Unidad de TI de la Entidad, en la medida de sus posibilidades, debe apoyar los mecanismos de pago en línea, en el momento que la Entidad determina ofrecer el servicio de pagos Electrónicos.

4.8 Acceso sencillo y eficaz de la información pública

Norma: La 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. Debe utilizar, en la medida de lo posible, esquemas de doble autenticación para evitar el acceso no autorizado a la información.

El Portal Oficial de Datos Abiertos de Panamá, administrado por la AIG, está disponible para la publicación del catálogo de datos abiertos de la Entidad y que son del interés público.

4.9 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, entre otros, que por disposiciones legales o reglamentarias establecen que deben ser publicadas en el tablero de anuncios de la institución.

4.10 Facilidad para las Personas con Discapacidad (PCD) o Personas en Situación de Discapacidad.

Norma: La Entidad deberá facilitar a los usuarios con discapacidad 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.

4.11 Facilitar el acceso e intercambio de información entre Entidades Públicas.

Norma: La Unidad de TI de la Entidad, en la medida de sus posibilidades debe habilitar convenios, protocolos y/o mecanismos que permitan intercambiar los datos dentro de los procesos de trámites (interoperabilidad).

4.12 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, para verificar el cumplimiento de las Normas, Estándares y condiciones para el buen uso de los sistemas y equipos.

4.13 Plan de Sistemas

Norma: La Unidad de TI de la Entidad, debe elaborar su Plan Anual 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.

SECRETARÍA GENERAL AIG

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.

4.14 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 del año siguiente, conteniendo las Iniciativas de Modernización Tecnológica que sigan los lineamientos que emita la AIG, y que incluya la programación a corto (1 año), mediano (3 años) y largo plazo (5 años).

4.15 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 plan de los proyectos presupuestados y aprobados.

SECRETARÍA GENERAL AIG

5. Normas de Aplicación General

5.1 Unidad Ejecutora de Gobierno Digital

Norma: La 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 en el Plan Operativo Anual. Además, deberá adoptar y dar seguimiento a los lineamientos que defina la AIG.

La Entidad, a través de su 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: 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 proporcionar 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: uso distinto al que fue recolectado, daño, pérdida o modificación no autorizada.

Se recomienda que la Entidad que posea (un mínimo) de 500 funcionarios, debe contar con al menos un (1) profesional certificado en Seguridad de la Información.

La Entidad con más de 1,000 funcionarios debe contar con un mínimo dos (2) profesionales certificados de Seguridad de la Información.

SECRETARÍA GENERAL AIG

En las entidades que cuenten con una oficina especializada en temas de seguridad informática y mantengan un director de seguridad de la información o CISO por sus siglas en inglés ("Chief Information Security Officer"), le corresponderá a esta oficina el planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones afín de mejorar la seguridad de la información.

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 recomendados en cuanto a la seguridad de la información.

Se recomienda implementar la "Norma" ISO 27001 en la(s) área(s) de mejor utilidad para la Entidad. En sectores específicos, ya sea una dirección, departamento, oficina o dependencia. Bajo ciertas circunstancias, no tiene que implementarse en toda la Entidad.

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

5.4 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 informática sobre sistemas y redes deben ser reportados al Equipo Nacional de Respuestas a Incidentes de Seguridad de la Información del Estado (CSIRT Panamá). 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 institucional.
- 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.

5.5 Seguimiento a los Contratos de Tecnología

Norma: El área responsable en la Unidad de TI debe mantener como política, dar 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 estos.

SECRETARÍA GENERAL AIG

5.6 Gestión de Proyectos de TI

Norma: El área responsable en la Unidad de TI, debe realizar el seguimiento a los proyectos de TI, fundamentado en las mejores prácticas de administración de proyectos, de manera que se 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.

5.7 Regulaciones que afectan la Gestión de TI

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

5.8 Inventario general de TI

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

El inventario debe estar organizado con dos secciones principales:

- **Activos físicos de TI (equipos)**: donde se registrarán todos los equipos de la infraestructura TI. Este registro debe incluir al menos: equipo, marca, modelo, asignación numeral de Bienes Patrimoniales, ubicación física, usuario asignado y estado (por ejemplo: funcional, en reparación, dañado, descarte).
- **Activos de programas, aplicaciones y licenciamiento**: donde se registrarán todos los programas utilizados, sistemas operativos, bases de datos y demás. Este registro debe incluir al menos: nombre, marca, versión, ubicación física, cantidad de licencias, usuarios asignados, fecha de vencimiento.

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

SECRETARÍA GENERAL AIG

6. De la Unidad de TI

6.1 Cargos o Puestos en las Dependencias de Tecnología de la Información

Norma: Debe existir una descripción del cargo y función de cada miembro de la Unidad u Oficina de TI, y los funcionarios de TI deben tener pleno conocimiento de esta reseña.

Justificación: Definir las responsabilidades de cada funcionario para la correcta gestión de los sistemas y los resultados de los componentes de Gobierno Digital que utiliza la Entidad.

6.2 Segregación de funciones

Norma: El jefe de la Unidad de TI debe mantener un control en la asignación de responsabilidades a los colaboradores, tomando en consideración la segregación de funciones, es decir, una misma persona no debe estar facultado para ejecutar, autorizar, registrar y custodiar a la vez. El personal debe poder distinguir dónde parten sus funciones y responsabilidades, y dónde empiezan las funciones de sus compañeros de grupo, área o proceso.

Justificación: La segregación de funciones reduce la probabilidad de fraudes, errores, o irregularidades en los procesos y el procesamiento de datos, sean intencionales o de forma involuntaria. Asimismo, puede brindar asistencia en la protección de los activos de la Entidad.

6.3 Registro del personal de la Unidad de TI

Norma: Se recomienda llevar un registro actualizado de la información del personal técnico dentro de la Unidad de TI, incluyendo lo siguiente: nombre completo, número de identificación, área a la que pertenece, cargo y funciones.

Justificación: Contar con un control de los recursos asignados a la Unidad de TI.

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 las Normas 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 en 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 con 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 Establecimiento de métricas

Norma: Definir e implementar un conjunto de métricas alineadas a los objetivos y metas de cumplimiento en la Unidad de TI, que sirvan para evaluar los avances y el desempeño en la ejecución de la Agenda Digital Institucional, los Planes de Simplificación de Trámites y el Operativo Anual.

Se sugiere realizar la revisión de los indicadores y su cumplimiento al menos trimestralmente o a convenir por los líderes de la Unidad de TI.

Justificación: Medir y reportar el cumplimiento de los objetivos; controlar y mejorar los procesos de la Unidad de TI, permitiendo la mejora continua y los ajustes oportunos para el logro de los objetivos.

6.8 Revisión de cumplimiento

Norma: La gestión de riesgos, los procedimientos de seguridad y los controles en las operaciones de TI, deberán ser evaluados por lo menos una vez al año.

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

SECRETARÍA GENERAL AIG

7. Procedimientos en TI

7.1 Elaboración y prueba de los procedimientos de TI

Norma: Las actividades y servicios que realiza la Unidad de TI, (respaldos, configuración de servidores, corrección de errores, instalación de software, mesa de ayuda, otros), deben contar con un procedimiento para su ejecución.

Todo procedimiento debe ser sometido a un proceso de verificación o prueba y de ser posible, este lo realice la oficina de auditoría interna o un grupo multidisciplinario.

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

7.2 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, en un lugar seguro.

Justificación: Mantener documentado cada función o tarea de la Unidad de TI. Salvaguardar y mantener accesibles y actualizados los procedimientos de TI.

7.3 Aprobación de los Procedimientos, Políticas, otros de TI

Norma: Los Procedimientos de TI, las Políticas, los Estándares, las Mejores Prácticas y las 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 dependencia o similar.

Justificación: Garantizar que los procedimientos de Tecnología han sido normados , oficiales y puedan ser auditables.

7.4 Revisión y actualización de los procedimientos de TI

Norma: Los Manuales de Procedimientos de TI deben ser revisados y actualizados al menos una vez al año.

Justificación: Mantener la vigencia y uso de los procedimientos de TI.

8. Administración Integral del Riesgo

8.1 Administración del riesgo tecnológico.

Norma: En caso de no existir una oficina responsable del tema de riesgo tecnológico en la institución, la Unidad de TI, debe implementar una metodología para estimar la magnitud de los riesgos a los que se encuentra expuesta la institución y así poder administrar, prevenir y responder adecuadamente a las amenazas. Dicha metodología debe cubrir los procesos tecnológicos y los sistemas informáticos.

Se recomienda considerar los principios y guías de la Norma **ISO 31000 de Gestión de Riesgos**, en su versión vigente.

Justificación: Reducir el riesgo tecnológico a niveles aceptables.

8.2 Evaluación del riesgo tecnológico

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

El proceso de evaluación de riesgos involucra los siguientes pasos:

- Identificación del riesgo: encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a la Entidad lograr sus objetivos.
- Análisis del riesgo: comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo.
- Valoración del riesgo: comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional.

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

8.3 Tratamiento del riesgo

Norma: Para cada uno de los riesgos identificados se debe seleccionar, documentar e implementar opciones para abordar el riesgo. La selección de las opciones para el tratamiento del riesgo debe realizarse de acuerdo con los objetivos de la Entidad, los criterios del riesgo, los recursos disponibles, y tomando en cuenta a todas las partes interesadas.

Algunas opciones para tratar los riesgos son las siguientes:

- Evitar
- Aceptar
- Compartir
- Retener
- Transferir

SECRETARÍA GENERAL AIG

Una vez se tomen las decisiones de tratamiento del riesgo, se debe crear y documentar un Plan de Implementación que contenga como mínimo lo siguiente:

- Fundamento de la selección de las opciones de tratamiento del riesgo y sus beneficios esperados
- Acciones propuestas
- Recursos necesarios
- Medidas de desempeño
- Plazos previstos para la implementación

Justificación: Minimizar el impacto y probabilidad de los riesgos tecnológicos y operativos de TI.

8.4 Seguimiento y revisión

Norma: El encargado de la unidad de TI, debe realizar el seguimiento y revisión periódica de los riesgos identificados. Este proceso incluye las actividades de: planificar, recopilar y analizar la información, registrar los resultados y proporcionar retroalimentación.

Los resultados del seguimiento y la revisión deben incorporarse a todas las actividades de la gestión del desempeño, de medición y de informe de la organización.

Justificación: Asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso de administración de riesgos.

8.5 Registro e Informe

Norma: El proceso de la gestión del riesgo y sus resultados se deben documentar e informar a través de los mecanismos apropiados, proporcionando información para la toma de decisiones.

Justificación: Tener visibilidad de la madurez de la administración del riesgo del área de TI y mejorar la calidad del diálogo con las partes interesadas, y apoyar a la alta dirección y a los órganos de supervisión a cumplir sus responsabilidades respecto a este proceso.

9. Autorizaciones

9.1 Solicitud de Servicios a la Unidad de TI

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 designada evaluará la solicitud para su aprobación, ejecución y documentación o rechazo, en cuyo caso realizará 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.

9.2 Inspección de archivos en dispositivos institucionales

Norma: En la circunstancia de requerir la inspección del contenido de archivos almacenados en dispositivos de la Entidad, el jefe del área u oficina en la que se encuentra asignado el dispositivo, elevará por escrito 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.

Toda inspección debe constar con un informe a detalle del procedimiento realizado.

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

9.3 Traslado de dispositivos TIC

Norma: Los dispositivos TIC, tales como: servidores, módems, equipos de comunicaciones, entre otros, no deben ser transportados sino cuentan con la autorización por escrito de la Unidad de TI, además se debe 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 estos.

9.4 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.

9.5 Privilegios y derechos de usuarios en servidores y sistemas institucionales

Norma: Debe establecerse un procedimiento para realizar las asignaciones y privilegios a los funcionarios con 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.

SECRETARÍA GENERAL AIG

Los accesos deben ser auditados periódicamente por el funcionario a cargo de seguridad informática de la Entidad, presentando un informe de cada revisión. Debe incluir la depuración y/o actualización de los privilegios y derechos de usuarios en base al listado actualizado de colaboradores de la Entidad.

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

SECRETARIA GENERAL AIG

10. Gestión de Licencias de Software

10.1 Adquisición de programas informáticos

Norma: El área responsable en la Unidad de TI, es el ente competente para realizar las recomendaciones, evaluaciones y controles, en 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 solicitado 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. Para las contrataciones que involucren tecnología de la información y la comunicación, cuyo monto sea superior a cincuenta mil balboas (B/. 50,000.00), la entidad deberá realizar una solicitud a través del Sistema de Evaluación de Solicitudes (SES) de la AIG. Adicionalmente la Unidad de TI, debe asegurarse que la iniciativa esté consignada en la Agenda Digital Institucional y en el Plan de Sistemas que se presentan ante la AIG, salvo se 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.

10.2 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 programa o aplicación (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.

10.3 Inventario de las licencias de los programas informáticos

Norma: El área responsable en la Unidad de TI, debe mantener un inventario de las licencias de programas y servicios 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.
- **Código SKU:** es el código de artículo del producto, este identificador lo proporciona el proveedor o fabricante.
- **Nombre de licencia:** es el identificador descriptivo de la licencia, se recomienda colocar el nombre como aparece en el catálogo del proveedor.
- **Versión:** es la especificación de la versión de la licencia.

- **Cantidad:** se recomienda llevar el control de la cantidad de licencias adquiridas, asignadas o utilizadas y disponibles.
- **Fecha de compra:** es la fecha efectiva en la cual entró en vigor la licencia, por lo general, es la misma fecha que se indica en el contrato.
- **Fecha de vencimiento:** es la fecha estipulada como fin del contrato celebrado al momento de la adquisición de las licencias.
- **Fecha de renovación:** se sugiere colocar una fecha previa (5 meses antes) a la de vencimiento como recordatorio para iniciar la gestión necesaria de renovación.
- **Número de contrato o factura:** es el número del contrato o factura celebrado al momento de la adquisición de las licencias.

Justificación: Establecer el ente responsable de la administración del licenciamiento de los programas y servicios informáticos en la Entidad.

10.4 Derechos de Propiedad Intelectual de las 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 Contrato, y se documenta las excepciones que se establezcan.

Todos los activos de información deben ser gestionados y monitoreados por la Unidad de TI quien será la responsable de la custodia e inventario.

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 y en base a los requerimientos institucionales.

10.5 Instalación y desinstalación de programas informáticos

Norma: Al momento de solicitar la asignación de 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. El encargado de la Unidad de TI debe verificar la disponibilidad de las licencias y actualizar el inventario de éstas una vez asignadas, antes de realizar la instalación.

En caso de requerir instalación de licencias en servidores o en otros equipos tecnológicos que conforman la infraestructura de TI, se recomienda hacer la solicitud formal a través del proceso de administración de cambios en producción establecido.

Se debe restringir a los usuarios finales de la Entidad, la instalación o desinstalación de programas en los equipos de cómputo.

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

10.6 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 informáticos con la finalidad de identificar las aplicaciones no autorizadas. Se recomienda realizar la verificación mensualmente.

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

10.7 Renovación y/o Actualización de los programas informáticos y aplicaciones

Norma: Se recomienda que la Entidad al momento de la adquisición de licencias o programas, incluya en el contrato las renovaciones y/o 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 que regula la contratación pública.

Las solicitudes de renovación, con monto mayor a cincuenta mil balboas (B/. 50,000.00), deben ser presentadas con anticipación de por lo menos 5 meses antes de su vencimiento, a través de la plataforma SES de la AIG.

Justificación: Mantener los activos tecnológicos actualizados y realizar las 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.

11. Adquisición y mantenimiento de la infraestructura tecnológica

11.1 Evaluación, recomendación y controles para la adquisición de infraestructura tecnológica

Norma: El área responsable dentro de la Unidad de TI estará a cargo de efectuar las evaluaciones, recomendaciones y controles en la adquisición de bienes y servicios tecnológicos, dentro de la Entidad. Adicional, las contrataciones que involucren tecnología de la información y la comunicación, cuyo monto sea superior a cincuenta mil balboas (B/. 50,000.00) deberán aplicar la normativa a través del Sistema de Evaluación de Solicitudes (SES) de la AIG 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 que una sola instancia actúe como ente responsable y encargado de la evaluación de los bienes y servicios tecnológicos dentro de las entidades.

11.2 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 examine 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.

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.

11.3 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.

La Unidad de TI debe solicitar a las diferentes direcciones o secretarias dentro de la Entidad que requieran implementar nuevos sistemas o aplicativos, los requisitos en cuanto a infraestructura para su desarrollo y así verificar si determinado hardware requiere ser actualizado.

Justificación: Actualización para la operatividad de los sistemas y reducir riesgos informáticos. Evitar la obsolescencia tecnológica en la Entidad.

11.4 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

SECRETARÍA GENERAL AIG

Cableado Estructurado, 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 sus versiones, bandas y frecuencias (IEEE 802.11x, WiFi, Bluetooth, etc.), manteniendo la debida configuración, restricción, acceso y seguridad apropiada.

Justificación: Garantizar la correcta operación y seguridad de los servicios de telecomunicación aplicando las buenas prácticas y normas para redes de comunicaciones.

11.5 Contratación de terceros para la implementación y el 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 opten por recurrir a la contratación de terceros, se recomienda establecer un 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.

Al adquirir nueva infraestructura tecnológica, la Entidad debe asegurarse de contratar los servicios de garantías extendidas de al menos 1 año, que incluya partes y mano de obra (mantenimiento) sin ningún costo adicional durante la vigencia del contrato. La Entidad debe gestionar la renovación del contrato con al menos 5 meses de anticipación a la fecha de terminación del servicio contratado.

Justificación: Aseguramiento de la calidad del entregable contratado y su sostenibilidad. Garantizar la continuidad y la alta disponibilidad de los servicios.

11.6 Tercerización de Administración y Gestión de Servidores

Norma: En el caso que la Entidad establezca un contrato para la tercerización o subcontratación de servicios para la administración y gestión de servidores, el personal del área responsable en la Unidad de TI debe solicitar un informe periódico de evaluación de los servidores en alcance, a la empresa contratada.

Este informe podría considerar entre otros puntos:

- Evaluación de riesgo
- Evaluación de seguridad informática
- Evaluación de licenciamiento
- Evaluación de sistemas de base de datos
- Evaluación de sistemas existentes

Justificación: Mantener el control de los trabajos realizados por los proveedores en la gestión de los servidores.

SECRETARÍA GENERAL AIG

12. Administración de la infraestructura de servidores

12.1 Control de acceso a la sala 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 debe firmar el registro de Entrada/Salida.

Si no es funcionario de la Entidad, el visitante debe estar acompañado por personal de tecnología, quien se encargará de supervisar su estadía dentro del área.

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

12.2 Privilegios en los servidores

Norma: Se debe controlar y limitar el acceso lógico y privilegios al personal de TI que utilice 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 estos. 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.

12.3 Administración proactiva

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

Para cumplir con esta responsabilidad, se recomienda 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.

Para esto se puede implementar herramientas para el monitoreo de las capacidades TIC y llevar una bitácora que registre las revisiones y evaluaciones de cualquier incidente que se haya registrado.

Justificación: Identificar posibles problemas de manera proactiva y así poder brindar una solución oportuna y eficaz para mantener las plataformas tecnológicas en óptimas condiciones y 99 % operativas.

12.4 Ubicación y condiciones de las salas de servidores

Norma: Todos los equipos, deben estar ubicados dentro de la(s) sala(s) de servidores o centro de procesamiento de datos, y los mismos deben estar alojados en gabinetes (racks), y se debe considerar la utilización de piso falso y contar con un ambiente controlado que ayude a detectar y disminuir la ocurrencia de eventos que puedan afectar el ambiente requerido, así como estar ubicado en áreas resguardadas, alejadas de fuentes de suministro de agua o aspersores de agua contra incendios que puedan afectar los equipos tecnológicos.

Adicionalmente las salas de servidores o de procesamientos de datos no deberán ser utilizadas en ningún momento como depósito para almacenar artículos de limpieza, cajas de cartón u otros objetos.

Deben contar con los siguientes Sistemas de Control:

- Sistema de protección y detección de incendios (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: Proteger los servidores, así como establecer los mecanismos de previsión y alerta que debe tener el área de servidores y equipos de comunicación.

12.5 Protección de los servidores contra condiciones eléctricas

Norma: Todos los equipos servidores deberán contar 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.

12.6 Bloqueo automático y doble autenticación en servidores

Norma: Cuando no se estén utilizando los servidores, sus pantallas deben permanecer bloqueadas con protectores de pantalla que no consuman recursos al sistema. Se recomienda habilitar la doble autenticación para la gestión de acceso a los servidores.

Justificación: Mantener la seguridad de los servidores impidiendo el acceso no autorizado y aumentar la seguridad de acceso a los sistemas operativos.

12.7 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.

SECRETARÍA GENERAL AIG

12.8 Actualizaciones

Norma: Los servidores en producción no deben estar configurados para realizar actualizaciones automáticamente. En su defecto, es necesario definir y documentar el procedimiento de actualizaciones de servidores, el cual deberá ser programado y controlado por la Unidad de TI y alineados con el proceso de administración de cambios en el ambiente de producción establecido.

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

13. Aplicaciones

13.1 Convenciones para el desarrollo de sistemas (software)

Norma: Para el desarrollo de aplicaciones se recomienda el uso de metodologías, para la gestión de proyectos, especialmente en el desarrollo de software y en otros entornos que requieren flexibilidad y adaptabilidad.

Para ello se sugiere la utilización de metodologías ágiles (SCRUM, KANBAN, LEAN), o similares para los desarrollos que incluyan los siguientes aspectos:

- Definición general de proyecto
- Realizar un estudio de viabilidad
- Definición y especificaciones de requerimientos
- Análisis de los riesgos asociados
- La estimación del costo del proyecto
- Asignación de recursos a las diferentes etapas del proyecto
- Diseño de modelo de datos
- Arquitectura de sistema
- Descripción de procesos y servicios ofrecidos por el sistema
- Documentación técnica API
- Proporcionar un marco de referencia de terminología y vocabulario común para el desarrollo del software.
- Procedimientos de instalación y prueba
- Documentación de implementación
- Acta de cierre de proyecto

Justificación: Alcanzar la uniformidad en la forma de gestión del desarrollo de las aplicaciones y permitir el establecimiento de las características operacionales de la aplicación (función, datos y procesos).

13.2 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 el mantenimiento a aplicaciones existentes, los Supervisores de Desarrollo y Seguridad Informática, además de ajustarse a lo solicitado por los usuarios funcionales, deben definir los aspectos de seguridad y accesos que requiere la aplicación. Esto debe ser realizado 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.
- En la integración y el desarrollo continuo de las aplicaciones, se recomienda la actualización continua y el control permanente del ciclo de vida del software.

Justificación: Establecer los controles de seguridad como una parte fundamental en el ciclo de vida del desarrollo de los sistemas.

13.3 Control de versiones en los Desarrollos de las Aplicaciones

Norma: Se recomienda que en el desarrollo de aplicaciones, se implemente un sistema de control de versiones, manteniendo un registro adecuado que permita un punto de restauración en caso de fallas.

Justificación: Mantener un control de actualizaciones de los sistemas en producción que permita mantener un histórico de todo el desarrollo del proyecto, como también la trazabilidad del desarrollo del software, ya que así se podrá ver qué cambios se han realizado en el código en cada versión.

13.4 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.

13.5 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.

13.6 Calidad de las aplicaciones

Norma: Para la comprobación de la calidad de las aplicaciones, se recomienda utilizar la familia del estándar ISO 25000 conocida como SQuaRE (System and Software Quality Requirements and Evaluation) es una familia de normas que tiene por objetivo la creación de un marco de trabajo común para evaluar la calidad del producto software y consta de cinco divisiones de calidad que son: gestión, modelo, medición, requisitos y evaluación.

Justificación: Proporcionar una estructura que permita medir la eficiencia y efectividad de la calidad de las aplicaciones.

SECRETARÍA GENERAL AIG

13.7 Pruebas a las aplicaciones

Norma: Se recomienda que la Unidad de TI encargada en el aseguramiento de la calidad de las aplicaciones realice las pruebas para comprobar el buen funcionamiento del software y detectar errores en el menor tiempo posible.

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

Los tipos de pruebas que se recomiendan aplicar son los siguientes:

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

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

13.8 Ambientes separados para desarrollo, 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.

13.9 Documentación de la operación y entrenamiento de la aplicación

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

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

SECRETARÍA GENERAL AIG

13.10 Sobre los Modelos utilizados en el desarrollo de aplicaciones

Norma: La arquitectura de software es un plan que define, cómo se estructuran y comunican los componentes de una aplicación y se centra en el desarrollo del esqueleto y la infraestructura general del software.

La arquitectura tradicional de ***cliente/servidor***, es conocida como una arquitectura de 2 capas: la capa que demanda una interfaz de usuario la cual se instala y se ejecuta en la Computadora Personal y la capa que envía las solicitudes al servidor que ejecuta las operaciones complejas.

La arquitectura de tres capas organiza las aplicaciones en tres capas lógicas:

1. La Capa de Presentación: La capa de presentación front-end es la parte de una aplicación que los usuarios ven y con la que interactúan.
2. La Capa de Aplicación: El back-end es la parte de una aplicación que no es visible al usuario, es la parte de una aplicación que procesa y almacena datos.
3. La Capa de Datos: Es un objeto que permite transferir información entre diferentes componentes de una aplicación o sitio web. Gestionar la base de datos, el almacenamiento y la recuperación de datos.

La AIG establece no utilizar arquitectura de 2 capas **cliente-servidor,** en los nuevos desarrollos de aplicaciones en plataformas estatales y se exhorta a utilizar la arquitectura y modelos de desarrollo de software como:

1. Modelo vista controlador (MVC)
2. Arquitectura orientada a eventos (EDA)
3. Arquitectura de Microservicios
4. Arquitectura en Capas (Multicapas)
5. Arquitectura Hexagonal (arquitectura de puertos y adaptadores)
6. Arquitectura orientada a servicios (SOA)
7. Framework (marco de trabajo)
8. Low-code y no-code: Permiten crear aplicaciones con poca codificación
9. DevOps: Integra los equipos de desarrollo y operaciones para una colaboración más estrecha
10. Modelo V también conocido como Modelo en V: Prioriza la documentación en cada fase de desarrollo
11. RAD (Rapid Application Development): Un modelo de construcción basado en elementos que se centra en el desarrollo rápido de aplicaciones

Justificación: Esta norma procura que se apliquen nuevas arquitecturas de software para los desarrollos de las aplicaciones en el Estado.

SECRETARÍA GENERAL AIG

14. Base de Datos

14.1 Responsabilidades, roles y perfiles del área de soporte a la Base de Datos

Norma: Los responsables por la administración, arquitectura, soporte operacional, calidad de los datos, disponibilidad de los datos, integraciones y otros aspectos técnicos, es el área de "Administración de Base de Datos". Para cumplir con su labor, deberá trabajar en cercana cooperación con los especialistas de infraestructura, seguridad, redes, sistemas operativos y aplicaciones.

Para el área de base de datos, se sugieren los siguientes perfiles como mínimo (roles y responsabilidades):

1. **Líder DBA**

Funciones:

- Responsable de gestionar, coordinar y planificar el departamento de base de datos, para la ejecución de las tareas operativas, técnicas y administrativas del área.
- Gestionar un equipo de especialistas, tales como: arquitecto de datos, DBA Junior y DBA Senior.
- Administrar, actualizar y aprobar, las políticas, procedimientos del área para monitoreo, soporte, seguridad, respaldos, permisos de accesos, gestión de datos y planificación de trabajos en base de datos.
- Administrar, mantener, actualizar y aprobar la documentación de los sistemas de base de datos, incluidas diccionario de datos, diagramas de entidad relación, diagramas lógicos, y físicos.
- Consultar a los usuarios para determinar las necesidades y asegurarse que las instalaciones cumplan con los requisitos del usuario o del proyecto.
- Proporcionar formación, apoyo y asesoramiento a los especialistas y usuarios.
- Mantenerse al día con las nuevas tecnologías.

2. **Arquitecto de base de datos**

Funciones:

- Diseña nuevas bases de datos, modelos de datos y estructuras para aplicaciones nuevas o existentes.
- Construir y mantener la arquitectura de la Base de Datos institucional y documentarla, lo que garantizará un mejor desempeño, flexibilidad, mantenibilidad, escalabilidad, seguridad, robustez y confiabilidad de los datos institucionales.
- Dar soporte al equipo procurando la aplicación de las mejores prácticas relacionadas al manejo de datos.
- Revisión de datos e integraciones (ETL, de las siglas en inglés "Extract, Transform and Load").
- Definir y gestionar el esquema del diccionario de datos. Especificar restricciones de integridad para asegurar los datos.
- Realizar el modelado de datos lógicos y traducir estos en un diseño de base de datos física.
- Analizar los requisitos de acceso a los datos para garantizar un diseño óptimo de la base de datos y un acceso SQL (de las siglas en inglés "Structure Query Language") eficiente.

- Creación y/o actualización de las políticas, procedimientos y estrategias de datos, respaldo y recuperación para las bases de datos.
- Investigar nuevas herramientas, evaluar tecnologías que aporten mejoras al área de base de datos y proponerlas al equipo y superiores.

3. **DBA Junior**

Funciones:

- Optimizar las consultas de SQL, procedimientos, funciones, disparadores, y reportes para un uso óptimo de las bases de datos y aplicaciones conectadas.
- Monitoreo permanente de servidores de base de datos, para asegurar su buen uso y funcionamiento en cuanto al rendimiento (CPU, Disco, procesos, sesiones, tareas programadas entre otros).
- Crear, revisar y auditar las sesiones de usuarios, roles, permisos y accesos a la base de datos.
- Administración y gestión de respaldos de Bases de Datos.
- Verificación de los datos generados desde las aplicaciones, procesos de respaldos, migraciones y reprocesar datos, para mantener la integridad de la información.
- Revisión de los procesos de respaldos, carga de datos, integridad de datos y verificaciones de la base de datos.
- Colaborar en confección de la documentación y actualización de políticas, proceso de migración de datos, normativas y/o estándares referentes a base de datos.
- Construir rutinas (script) para procesos de manipulación, definición, migración de datos, respaldos y mantenimientos de objetos.
- Investigar nuevas herramientas, evaluar tecnologías que aporten mejoras al área de base de datos y proponerlas al equipo y superiores.

4. **DBA Senior**

Funciones:

- Responsable de instalar, implementar los esquemas, configuración, parámetros, motores, objetos, estructuras y modelos dentro de un servidor de base de datos.
- Ajustes al sistema operativo del servidor, software de administración y procesos de hardware en la base de datos (memoria, discos y procesadores).
- Diseñar, implementar y desplegar los mecanismos y políticas para seguridad, monitoreo, soporte de los servidores de bases de datos.
- Monitoreo permanente de servidores de base de datos, para asegurar su buen uso y funcionamiento en cuanto a rendimiento y procesamientos (CPU, Disco, procesos, sesiones, tareas programadas, entre otros).
- Actualización a las nuevas versiones, aplicar correcciones, parches, y configuración de los parámetros del servidor de base de datos.
- Brindar mantenimiento al esquema del diccionario de datos.
- Diseñar, implementar y mantener las políticas de retención de datos y de almacenamiento.
- Desarrollo de tareas de mejoras de base de datos, en consultas, reportes, configuración del servidor y tareas de replicación.
- Dar soporte a la integración de aplicaciones de terceros.
- Desarrollar auditorías de usuarios (roles, perfiles y privilegios).

- Investigar nuevas herramientas, evaluar tecnologías que aporten mejoras al área de base de datos y proponerlas al equipo y superiores.

Justificación: Definir los roles, para la selección correcta del talento humano con un perfil debidamente calificado y cualificado, a fin de cumplir con los procesos, delimitar funciones, asignar sus responsabilidades, cumplir con misión y visión dentro de la Entidad.

14.2 Documentos físicos y digitales de la Base de Datos

Norma: El área de administradores de base de datos, deberá contar con la siguiente documentación, ya sea física o digital:

- El diagrama entidad relación
- Estructuración física y lógica
- Procedimientos y la descripción de las instancias: departamento que la utiliza, usuarios (nombre, privilegios).
- Licenciamientos vigentes
- Mantener los procedimientos, guías, lista de verificación y los procesos para la creación de Instancias, tablas, Índices, funciones, procedimientos almacenados, vistas y reportes que requiera un acceso a base de datos.
- Documentación para la gestión de cambios y versiones de los objetos de la base de datos.

Justificación: Mantener la documentación al día de los de las bases de datos, sus estructuras, objetos y procesos de control de cambios.

14.3 Documentación técnica de la Base de Datos (diccionarios)

Normas: Los responsables de la Unidad de TI, de aplicaciones y la base de datos, deben mantener la documentación técnica y el diccionario de datos actualizados y organizados con los nombres de las estructuras, sus definiciones, características, atributos lógicos, tipos de datos, la función de cada uno de los objetos de la base de datos y/o conjunto de datos

Justificación: Tener un lenguaje común entre los administradores de las bases de datos, programadores y los posibles usuarios que tendrán acceso a dichas estructuras al momento de implementar tareas o nuevas aplicaciones.

14.4 Gestión de cambios en Base de datos

Norma: Los responsables de TI en base de datos, deberán implementar los procedimientos para el control de cambios, configuración y gestión de versiones tanto para motores de la base de datos, sus estructuras de datos, tablas, configuración y procesos.

Para ello se recomienda llevar un proceso de control de cambios automatizado (software) o con el uso de listas de verificación documentados, que contenga la información del ítem a modificar, el impacto a nivel de aplicación, propósito del cambio solicitado, los responsables de la solicitud, el script de la modificación y el estado actual del objeto a modificar, así como las autorizaciones del área que solicita.

Serán los especialistas de DBA's los que deben cuidar la información suministrada y realizar las verificaciones en los ambientes de prueba, para determinar el impacto final de los cambios solicitados.

Justificación: Llevar un control de cambios y una gestión de la configuración eficiente, permite la sincronización de las estructuras en la base de datos, aplicaciones, lo cual disminuye los riesgos de errores, afectar la integridad de los datos, eficiencia en las implementaciones de los proyectos.

14.5 Realización de respaldos diarios a la Base de datos

Norma: El encargado de la base de datos, debe crear rutinas programables de respaldo que se ejecuten diariamente, (preferible en horas no laborables), Debe realizar pruebas de recuperación y restauración.

Las copias de respaldo se deben de almacenar en dispositivos (ejemplo servidores de back-ups, cintas magnéticas entre otros) y se almacenados en un sitio con control de acceso.

Se recomienda que la Entidad tenga dos respaldos y que sean almacenados en distintos recintos por si existen algún tipo de riesgo (naturales, alteraciones y físicos).

Justificación: Mitigar los riesgos manteniendo el control y respaldos de la información garantizando la continuidad de la operación.

14.6 Planificación de los procesos de depuración de datos y administración de espacio en disco

Norma: Los responsables de TI para la administración de la base de datos, deberán establecer las políticas de limpieza de datos, compresión de datos, integridad de datos, tiempo en discos de los datos y administración de espacio en disco, para de esta forma gestionar el creciente volumen de información, discos, periodicidad en que los datos estarán en la base de datos.

Justificación: Con el establecimiento de una estrategia de depuración de datos y administración de discos, se garantiza integridad de los datos, la carga de datos, capacidad de procesamiento, disponibilidad de datos históricos para auditoria, ahorros en costos de espacio en servidor y de esta forma mantener alta disponibilidad de la información para los usuarios y aplicaciones.

14.7 Gestión de la seguridad, integridad, accesos a aplicaciones y control de usuarios en Bases de Datos

Norma: Serán responsabilidad del grupo de administradores de base de datos (DBA's), velar por el cumplimiento de los controles y prácticas tales como:

- Cumplimiento de las políticas de la organización
- Seguridad de cuentas de usuarios (roles)
- Instalación y/o actualización de parches de seguridad
- Implementación del cifrado de datos

- Seguridad de la copia de respaldo
- Auditoria de datos, procesos, dispositivos y usuarios que se conectan a la base de datos.
- Control de aplicaciones que se conectan a la base de datos
- Comprobación de la integridad de los datos

Justificación: Mantener la seguridad, disponibilidad, privacidad, control, autenticidad y aplicar las medidas de protección necesarias para evitar la pérdida y accesos no autorizados a datos.

14.8 Procesos de monitoreo

Norma: La Unidad de TI encargada de la administración de las bases de datos debe contar con software y/o herramientas para la gestión de las base de datos, permitiendo realizar el monitoreo, diagnósticos, soporte a problemas, revisión del rendimiento, colectar estadísticas, optimizar y visualizar los esquemas lógicos de base de datos, para brindar un soporte adecuado en caso de fallos, investigar problemas, y crear reportes.

Entre las recomendaciones de herramientas de monitoreo (software libre o bajo licencia), se pueden mencionar:

- Nagios Database Monitoring (software libre)
- Grafana (software libre)
- PRTG Monitoring Database
- Oracle Cloud Control
- SQL Server Management Studio
- Quest Database Management
- SolarWinds Database Performance Analyzer
- DB Artisan Database Administration Solution

Justificación: Monitorear, medir el desempeño y rendimiento de las bases de datos, que brindarán apoyo en la implementación de acciones preventivas y correctivas para mantener los servicios de base de datos disponibles y satisfacer las demandas de información.

14.9 Configuración y mantenimiento de base de datos

Norma: Es la Unidad de TI, a través del administrador de BD, la encargada de gestionar el servidor y la configuración de espacios y esquemas de la base de datos. Esto incluye instalación y actualización del software y motor de base de datos, documentación, monitoreo de conexiones, memoria, procesos, optimización y planificación de las necesidades previstas de recursos para la base de datos.

Para realizar estas actualizaciones y darle un mayor desempeño a la base de datos, se recomienda:

- **Copias de Seguridad:** comprobar las copias de seguridad para validar que se crearon correctamente según su proceso.
- **Procesamiento Nocturno:** revisar los procesos nocturnos o de madrugada.

- **Registro de Errores:** revisar el registro de errores de SQL Server en busca de errores o problemas de seguridad inesperados (inicios de sesión exitosos o fallidos).
- **Registro de Sucesos de Windows:** revisar el registro de sucesos de aplicaciones al mínimo para averiguar si se están escribiendo errores o advertencias relacionados con Windows o hardware.
- **Trabajos de Agente SQL Server:** monitorear y revisar de las ejecuciones del SQL Server Agent, de las tareas programados y revisar las ejecuciones fallidas.
- **Registros de Alta Disponibilidad y/o Recuperación de Desastres:** comprobar los registros de proceso de alta disponibilidad y/o recuperación de desastres. Dependiendo de la solución que se está usando (Log Shipping, Clustering, Replication, Database Mirroring, CDP, etc.) dicta lo que se debe comprobar.
- **Registros de Rendimiento:** revisar las métricas de rendimiento para determinar si se superó su línea de base o si tuvo puntos lentos durante el día que deben revisarse.
- **Registros de Seguridad:** revisar los registros de seguridad de una solución de terceros o de los registros de errores de SQL para determinar si tuvo una infracción en una de sus políticas.
- **Manejo Centralizado de Errores:** si se tiene una aplicación, por registro de SQL Server o de nivel empresarial, revisar esos registros para detectar cualquier error inesperado.
- **Almacenamiento:** validar que se tiene suficiente espacio de almacenamiento en sus unidades para soportar sus bases de datos, copias de seguridad, procesos por lotes, etc. a corto plazo.

Justificación: Garantizar una revisión y mantenimiento periódico de la Base de Datos.

14.10 Migraciones y replicación de datos y base de datos (internas/externas)

Norma: Las migraciones y replicaciones de datos y base de datos, deben ser solicitadas al área de base de datos formalmente por escrito y ésta debe ser revisada para evaluar su viabilidad. Estas migraciones y replicaciones deben ser gestionadas y ejecutadas por el personal de administración de base de datos (DBA's) de la Unidad de TI.

Presentar un plan del proyecto con tiempos definidos de migración/replicación, tomando en cuenta aspectos relevantes como: identificar las fuentes de datos a migrar, identificar las estructuras diseñadas para almacenar los datos, observar el formato que tienen los datos con el objetivo de identificar las conversiones necesarias para adaptarse a las nuevas necesidades, realizar pruebas previas a la migración con el fin de identificar oportunamente las excepciones presentes propiamente en las estructuras y datos actuales que pudiesen surgir en el proceso de la migración.

Justificación: Asegurar el proceso de migración y replicación de base de datos, estructura de datos, tiempos, recursos digitales, fuentes de datos, almacenamiento y que el personal técnico esté organizado, asegurando una exitosa tarea de migración.

15. Monitoreo de las bitácoras

15.1 Eventos del Sistema

Norma: Todo sistema operativo debe contar con una herramienta para la observación (monitoreo) y registro de la ocurrencia de los eventos del sistema operativo, principalmente los de seguridad.

Ejemplo de algunas herramientas más conocidas para este tipo de análisis (software libre)

- Para UNIX/Linux: Logcheck y SWATCH.
- Para Windows: LogAgent, NetView, Solarwinds

Al utilizar herramientas que no requieren el pago de licenciamiento, se debe gestionar con antelación a la descarga e instalación, con el encargado de la Unidad de TI para recibir autorización de descargas de software no licenciados en equipos informáticos de la Entidad.

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

15.2 Bitácoras para el manejo de información confidencial

Norma: Todos los sistemas en producción y que procesen información confidencial, deben generar un registro en bitácora al momento de realizar operaciones de inserción, modificación o eliminación. Ese registro debe incluir al menos:

- Dirección IP del dispositivo
- Dirección MAC
- Fecha y hora de la acción
- Nombre de usuario
- Nombre de la aplicación
- Registro histórico
- Registro actual

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

15.3 Período de retención de las bitácoras del sistema

Norma: Las bitácoras relacionadas a los eventos de seguridad, deben mantenerse por un período mínimo de noventa (90) días (es la recomendación), en el sistema. Luego del período indicado, el encargado de sistemas debe depositar las bitácoras en un medio de almacenamiento en un lugar seguro.

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

15.4 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 auditorías, 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.

15.5 Desarrollo de Rutinas de Bitácora

Norma: El encargado de la Unidad de TI, debe programar rutinas para la automatización de la bitácora, con el fin de elaborar informes de las acciones generadas en los sistemas, ante incidentes de seguridad, detección de comportamiento inusual, información para resolver problemas y realizar mejora continua.

Ejemplos de rutinas de bitácoras para proteger la información de la Entidad:

- Messages
- Xferlog
- Wtmp
- Secure
- Lastlog
- Maillog
- Access_log
- Dmesg

Justificación: Establecer la automatización de informes en las bitácoras, para mantener un control de la calidad de los sistemas y mitigar los riesgos de la información.

15.6 Revisión regular de las bitácoras del sistema

Norma: Se debe revisar diariamente las bitácoras monitoreando la información de los registros 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.

16. Administración de cambios en el ambiente de producción

16.1 La administración de cambios debe ser parte de un procedimiento formal

Norma: Debe existir un procedimiento formal y por escrito, para la gestión de las solicitudes de cambios en aplicaciones, la infraestructura, datos, seguridad, y otros componentes de TI que puedan afectar la continuidad de los servicios.

Se recomienda definir un procedimiento de acuerdo con el tipo de cambio que se desea realizar:

- Cambios estándares
- Cambios normales
- Cambios de emergencia

Justificación: Requerir el uso de un procedimiento formal y por escrito, para llevar y mantener un control de los cambios en el ambiente de producción.

16.2 Evaluación de solicitudes de cambios en producción

Norma: Las solicitudes para cambios en los sistemas o aplicaciones en producción deben ser evaluadas por los encargados de la unidad de TI quienes tomarán la decisión si se autoriza el cambio y seleccionar una ventana de tiempo para la aplicación de los cambios, y que en lo posible que no afecte la disponibilidad de los servicios. Los resultados de la evaluación deben quedar documentados.

En esta evaluación puede participar personal de negocio si es requerido.

Se recomienda tomar las siguientes consideraciones al momento de evaluar una solicitud de cambio:

- Plan de trabajo: existencia de una lista de actividades claves para la ejecución y validación del cambio y su asignación de recursos.
- Motivo del cambio
- Análisis de riesgos
- Evidencia de pruebas (aplica para cambios de desarrollo, parches, actualizaciones, cambios de datos).
- Plan de rollback (reversión): existencia de un plan para retornar a la versión o estado anterior al cambio en caso de que el cambio falle.
- Artefactos en alcance: tener claridad sobre los componentes que se afectarán o pueden afectarse al realizar el cambio.

Justificación: Asegurar un control adecuado de los cambios en producción, aumentar las probabilidades de éxito de estos y garantizar la continuidad de los servicios.

16.3 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.

16.4 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 departamento afectado deberá 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 con los procedimientos establecidos. Se debe mantener en respaldo los datos antes y después de la corrección. Una vez ejecutado el cambio se requiere una confirmación de satisfacción por escrito por parte del solicitante.

Si el problema es recurrente debe automatizarse la funcionalidad y asignarla al usuario final autorizado.

Justificación: Proteger la integridad de datos en producción.

16.5 Instalación de actualizaciones

Norma: Vigilar y monitorear periódicamente las actualizaciones ofrecidas por los propios desarrolladores y fabricantes de las aplicaciones, y aplicar oportunamente las últimas actualizaciones, parches o mejoras a los equipos, servidores o aplicaciones en producción. Los encargados de la Unidad de TI serán los responsables directos de esta actividad.

Se recomienda que estas actualizaciones sean aplicadas en un ambiente de prueba, 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, de acuerdo con el procedimiento formal establecido.

Estas actualizaciones se ejecutarán en sitio o de manera remota de acuerdo con la criticidad del cambio y se acordará con el usuario la realización de éste, para no afectar las actividades diarias de los usuarios.

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

16.6 Seguimiento a los cambios post-producción

Norma: Después de la ejecución de los cambios en producción, se recomienda realizar pruebas de validación de los cambios y realizar monitoreo de los servicios por el tiempo establecido en la evaluación de las solicitudes de cambio. Debe quedar documentación de las pruebas y resultado del monitoreo como evidencia para dar por finalizado el cambio.

Justificación: Garantizar que los cambios en producción se hayan efectuado satisfactoriamente y no haya afectación de los servicios.

16.7 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 realizadas en las aplicaciones o sistemas informáticos.

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

16.8 Documentación de las modificaciones realizadas a la aplicación

Norma: Se debe mantener la documentación que refleje 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.

16.9 Acceso del personal de desarrollo al ambiente en producción

Norma: El personal que participa en el desarrollo de aplicaciones o sistemas, no debe tener acceso a los sistemas en producción. La única excepción en donde se puede dar acceso controlado y con presencia de supervisor de seguridad informática y/o auditoría interna será para la atención de incidentes críticos previa autorización. Estos accesos y cambios que se realicen en producción deben quedar registrados en bitácora.

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

16.10 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.

17. Niveles del Servicio Técnico y relaciones con terceros

17.1 Primer nivel de servicio

Norma: Los funcionarios que requieran soporte técnico y/o ayuda en procedimientos, podrán recibirlo a través de la Mesa de Ayuda de soporte de nivel 1 de la Unidad de TI o mediante servicio contratado a terceros. En caso de que la solución a la solicitud del funcionario esté fuera del alcance de este nivel, el requerimiento será transferido al nivel 2 de servicio.

Justificación: Informar a los usuarios acerca de la metodología o pasos a seguir al momento de requerir asistencia y/o soporte técnico.

17.2 Segundo nivel de servicio

Norma: El nivel 2 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.

17.3 Tercer nivel de servicio a los

Norma: El nivel 3 de servicio, se refiere a la situación en que el personal de Soporte Técnico de la entidad no puede atender la solicitud y esta se canalizaran a los proveedores externos de las soluciones tecnológicas de la Entidad. Para esto, se deberá contar previamente con contratos de servicios con los proveedores (SLA, de las siglas en inglés "Service Level Agreement") y así garantizar un tiempo de respuesta aceptable a las solicitudes.

Justificación: Establecer el alcance de los niveles del servicio técnico.

17.4 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. Esta cláusula deberá estar firmada por el representante legal del proveedor.

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

17.5 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 asignar a una persona dentro de la Unidad de TI, para que aplique el debido seguimiento y garantice el retorno del bien o bienes en la fecha estipulada y en el mismo estado que fueron entregados.

Justificación: Mantener un control estricto de los bienes que pertenecen al Estado y que estén siendo utilizados por personal ajeno a la Entidad.

SECRETARÍA GENERAL AIG

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

Norma: En el momento que un proveedor, especialista, o contratista culmine su relación con la Entidad y posea bienes tecnológicos propiedad del Estado, estos deben ser reintegrados a la Entidad. Los 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 revocar los privilegios en los sistemas computacionales, 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: Reintegrar los bienes a lo cual tuvo posesión un proveedor, además de controlar los derechos y privilegios en los sistemas de información para salvaguardar los bienes e información del Estado.

17.7 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 sus equipos 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 el uso de equipos no pertenecientes 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.

17.8 Utilización de Internet de la Entidad, por parte de proveedores o visitantes

Norma: Todo proveedor que requiera acceso a Internet desde las premisas de la Entidad, debe contar con un plan de datos que le proporcione su empresa para no incurrir en solicitudes o permisos para utilizar la red Internet de la Entidad. En caso de requerir actualizar sistemas o software en equipos específicos contratados con la Entidad y que estos archivos sean de gran tamaño, deberá solicitar se le asigne un computador de la Unidad de TI para realizar esta labor sin incurrir en accesos no autorizados.

Justificación: Ir aplicando de manera gradual o escalonada, políticas en cuanto a modelos o marcos actuales en ciberseguridad tales como el concepto denominado "Zero Trust" o "Confianza Cero".

SECRETARÍA GENERAL AIG

18. Continuidad del servicio

18.1 Gestión de la Continuidad de los Servicios de TI

Norma: El área responsable en la Unidad de TI, debe adoptar una metodología para la Gestión de la Continuidad del Servicio, para lo cual recomendamos consideren el apartado **Gestión de la Continuidad de Servicios (ITSCM)** de la Biblioteca de Infraestructura de Tecnologías de Información (ITIL) versión 4 o versión vigente.

Adicional, puede utilizar la Norma **ISO/IEC 27031:2011** Guías para la preparación de las tecnologías de información y comunicaciones para la continuidad del negocio, en su versión vigente. La ISO 27031 es un estándar especializado que aborda la continuidad del negocio con ISO 22301 asumiendo la actividad detallada desde allí. ISO 22301 es el estándar internacional que ayuda a las organizaciones a protegerse y recuperarse de incidentes disruptivos cuando ocurren.

El propósito de la práctica de gestión de la continuidad del servicio es garantizar que la disponibilidad y el rendimiento de un servicio se mantengan en niveles suficientes en caso de desastre.

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

18.2 Preparación y mantenimiento de un Plan de Contingencia

Norma: La Entidad debe poseer un Plan de Contingencia para la continuidad de sus operaciones informáticas, 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 por escenario 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.

18.3 Implementación de un Plan de Recuperación de Desastres

Norma: Para la implementación del Plan de Recuperación de Desastres (DRP), se recomienda la participación tanto de personal de TI como de negocio, y 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 (tiempo objetivo de recuperación)
- RPO (punto objetivo 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.

18.4 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.

18.5 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 los sistemas y la información, en caso de incidentes, afectando lo menos posible los servicios.

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

18.6 Topología de red y Diagramas de interconexión

Norma: La Unidad de TI debe poseer diagramas de la topología de física y lógica (localización y especificaciones técnicas de los puntos de acceso, routers, switches, firewalls, líneas con los proveedores de Internet); así como también mantenga los archivos de configuración de los equipos que conforman la red (switches y routers) de la Entidad.

Todos los documentos que mantengan información sobre de red, deben ser almacenados de forma segura, ya sea que esté impresa o en línea en un servidor con permisos restringidos.

Justificación: Permitir el diagnóstico y resolución de los problemas de la red de manera eficiente.

SECRETARÍA GENERAL AIG

19. Custodia de Datos por Terceros

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

Norma: La Unidad de TI debe asegurarse que el contrato suscrito para la prestación de los servicios señalados contenga cláusulas que comprometan a la empresa contratada a realizar una 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 y/o archivos de la Entidad, durante y posterior a la finalización de la relación contractual.

19.2 Principios Generales para la Custodia de datos por Terceros

Norma: El proveedor deberá proteger el entorno tecnológico y los datos alojados de la Entidad. Debe entregar informes del cumplimiento de administración, supervisión y gestión de datos seguros.

Justificación: Mantener la integridad de los datos basados en una relación de confianza con el proveedor de servicios.

19.3 Acuerdo de Confidencialidad sobre la información

Norma: La Unidad de TI debe asegurarse que se establezcan cláusulas dentro del contrato o se constituya un Acuerdo de Confidencialidad con las empresas, relacionadas 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.

19.4 Revisión anual de los procedimientos para la custodia de datos por Terceros

Norma: La Unidad de TI debe de realizar cada año, revisiones a los procedimientos de gestión y transferencia segura de datos de la Entidad, para mantener actualizada la metodología de supervisión y vigilancia interna y/o externa, incluyendo las auditorías.

Justificación: Mantener la integridad de los datos y comprobar el cumplimento de las políticas

19.5 Registro de acceso y auditoría para la custodia de datos por terceros

Norma: Se recomienda a la Unidad de TI, implementar controles que permitan realizar auditorías del acceso a documentos y/o archivos, tanto digitales como físicos, con el fin de alcanzar transparencia en las operaciones de resguardos de la información.

Justificación: Prevención de acceso no autorizado a la información.

19.6 Recuperación de información custodiada por terceros

Normas: La Unidad de TI deberá tener políticas documentadas de los procedimientos de recuperación de información con técnicas forenses y generación de informe relacionados con riesgos.

Justificación: Reducir el riesgo de pérdida de datos.

SECRETARÍA GENERAL AIG

19.7 Procedimientos para la eliminación de datos custodiados por terceros

Norma: El encargado de la Unidad de TI debe asegurarse que se produzca la documentación del procedimiento de destrucción segura de la información, que se encuentren almacenada en dispositivos electrónicos (ejemplo: cintas magnéticas, medios ópticos, entre otros) en custodia de terceros.

Justificación: Garantizar que los datos sean eliminados correctamente, con el fin de que ningún intermediario no involucrado en el proceso, acceda a información confidencial de la Entidad.

SECRETARÍA GENERAL AIG

20. Uso y manejo de la información

20.1 La Información como Activo

Norma: La información es considerada un activo del Estado. La Entidad es la responsable por el resguardo de los activos de información: documentos digitales, bases de datos, archivos, aplicaciones informáticas, 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.

20.2 Clasificación de información

Norma: Para los efectos de aplicación e interpretación en materia de clasificación de información en las entidades, recomendamos utilizar como referencia, lo establecido en la Ley 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.º 1 numeral 4, 5, 6 y 7.

- **Información:** Todo tipo de dato contenido en cualquier medio, documento o registro impreso, óptico, electrónico; químico, físico o biológico.
- **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 de cualquier Entidad pública que no tenga restricción.
- **Información de Acceso Restringido:** Todo tipo de información de cualquiera Entidad, cuya divulgación haya sido restringida únicamente a los funcionarios que la deban conocer a razón de sus facultades, de acuerdo con la Ley.

Recomendamos que la información sea utilizada dentro sus niveles de clasificación.

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

20.3 Confidencialidad de la información

Norma: Los activos de información clasificados 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.

Si existen indicios que la información confidencial o restringida alojada en los equipos informáticos ha sido revelada a una persona no autorizada o ha sufrido algún tipo de pérdida de esta, el jefe de la Unidad de TI notificará al Director del área y al Despacho Superior de la Entidad.

Justificación: Proteger los datos con información confidencial mediante niveles de accesibilidad. Y tomar las medidas correctivas para evitar la pérdida o el robo de la información confidencial y que ésta sea utilizada en perjuicio del Estado o de los ciudadanos.

20.4 Retiro de información institucional de las instalaciones públicas

Norma: El funcionario tiene terminantemente prohibido retirar activos de información digital fuera de la Entidad. Si por razones de sus funciones tiene la necesidad de hacerlo, debe gestionar la autorización mediante solicitud escrita y firmada por el Despacho Superior, Director o Jefe que le asignó la tarea.

Justificación: Resguardar la información que es propiedad del Estado.

20.5 Acuerdo de confidencialidad de los funcionarios de tecnología

Norma: Se recomienda establecer un acuerdo de confidencialidad cuando se integre un funcionario a la Unidad de TI, en donde se comprometa a no divulgar información que ponga en riesgo la confidencialidad de los datos de la Entidad.

Justificación: Proteger y cuidar la información confidencial de la Entidad.

21. Confidencialidad

21.1 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.

21.2 Compromiso del funcionario con la seguridad de la información

Norma: Todo funcionario de la Entidad, 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 las campañas de concientización, salvo que otra dependencia 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.

21.3 Cifrado

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

Se recomienda a la Entidad utilizar controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante.

Justificación: Garantizar la confidencialidad de la información con mayor grado de seguridad en los canales de acceso de la Entidad.

21.4 Autorización para verificar los correos electrónicos en la Entidad

Norma: Es indebido que los funcionarios de la Unidad de TI inspeccionen los correos electrónicos de los funcionarios, salvo que se cuente con la autorización por escrito del Despacho Superior o que se trate de una investigación judicial.

Justificación: Evitar el acceso no autorizado a la información contenida en los correos electrónicos institucionales propiedad del Estado.

21.5 Análisis y monitoreo de la actividad en la red institucional e internet de la Entidad

Norma: El Oficial de Seguridad de la Unidad de TI o personal designado examinarán las actividades de los funcionarios en la red interna e Internet, solamente con el propósito de administrar los recursos y/o brindar soporte a investigaciones o auditorías.

Justificación: Aplicar control en el uso de los recursos y los lineamientos para de la red.

22. Gestión del perímetro de seguridad

22.1 Cortafuegos (Firewalls)

Norma: Se recomienda la instalación y configuración de un firewall, el cual puede ser implementado por hardware, como perímetro de entrada y como software para desarrollo y aplicativos webs. Éstos definen el tráfico de la red, sobre una base de conjuntos de políticas de seguridad para filtrar el ingreso de tráfico potencialmente peligroso o no autorizado en la red.

En las reglas deben considerar plantillas de configuración como: controles de acceso preventivos (autorizado y no autorizado), ACL (Lista de Control de Acceso), APP filtración del tráfico de aplicaciones, WAF (Web Application Firewall) y ADC (controlador de entrega de aplicaciones) en dispositivos, protocolos, puertos o servicios en la red.

Se recomienda que la configuración del WAF use el método multicapa y detención correlacionada.

Justificación: Contar con un equipo de seguridad perimetral para la prevención de ataques o afectaciones a los sistemas de la Entidad. Bloquear el acceso no autorizado y prevención de ataques o afectaciones a los sistemas del Estado.

22.2 Sistema de Detección y Respuestas Gestionada a Amenazas (MDR)

Norma: Se recomienda que las entidades tengan soluciones MDR (Managed Detection and Response, por sus siglas en ingles), para prevenir una amplia gama de amenazas. Dichas herramientas, de manera remota, proporcionan detección de amenazas y recomendaciones de respuesta, tanto en endpoints como en entornos de nube, híbridos y en las mismas instalaciones.

La MDR consiste en tres pasos: recolección, en el que se recopilan los datos de registro desde varios sistemas esenciales como endpoints, firewalls, enrutadores, sistemas de acceso remoto y varias plataformas en la nube; detección e investigación, en el que se buscan, de forma proactiva, indicadores de un ciberataque en curso, y respuesta, en el que se toman las medidas para responder a un evento de seguridad

La detección y respuesta gestionada o MDR, funciona mediante la integración de una plataforma de seguridad con inteligencia de amenazas, análisis avanzado y servicios profesionales dirigidos por expertos. Cada acrónimo tiene una funcionalidad única:

- La solución **EDR** (Detección y respuesta de punto final) Cada dispositivo conectado a una red representa un vector de ataque potencial para las amenazas de Internet, y cada una de estas conexiones es una puerta de entrada potencial a sus datos. En general, las soluciones EDR recopilan datos de los puntos finales, los cuales se utilizan para identificar amenazas potenciales y brindan formas útiles de investigar y responder a esas amenazas potenciales.
- La solución **NDR** (Detección y respuesta de red) que están diseñadas para detectar amenazas cibernéticas en redes corporativas mediante el aprendizaje automático y el análisis de datos. Estas herramientas crean modelos de comportamiento normal

SECRETARÍA GENERAL AIG

mediante el análisis continuo del tráfico de red y luego utilizan estos modelos para identificar patrones de tráfico anómalos o sospechosos.

- La solución **XDR** (detección y respuesta extendidas) incorporan y analizan pasivamente datos de red multicapa y monitorean el tráfico. Esta categoría de solución generalmente aplica análisis de comportamiento avanzado junto con aprendizaje automático para detectar, investigar y responder rápidamente a amenazas.

Justificación: Establecer herramientas de Detección y Respuestas para la visibilidad en múltiples niveles de seguridad.

22.3 Sistemas de Prevención y Detección de Accesos (IPS/IDS)

Norma: Se recomienda la implementación de sistema de prevención y detección de intrusión la cual ayudará al monitoreo, revisión o revelar actividad sospechosa en el tráfico de la red de la Entidad y así responder a ataques e intrusiones posibles, además de grabar información histórica y generar reportes con las siguientes herramientas:

- Los sistemas de detección de intrusiones **(IDS)** supervisan de forma pasiva el tráfico en la red. Ayuda detectar los ataques y monitorear los flujos del tráfico, pero requiere la asistencia de otros dispositivos de red, como routers y firewalls, para responder a un ataque. Se toma como opción para la implementación de la seguridad, se une a otra herramienta que provee la protección de los servicios del sistema.

  Entre sus tareas principales están:

  - Prevenir usando sensores para monitorear el tráfico en la red e identificando reglas aplicadas a ataques.
  - Reaccionar detectando patrones de intrusión en rastros de los servicios de red o en el comportamiento del sistema.

- Los sistemas de prevención de intrusiones **(IPS)** detectan signos de ataques o de tráfico inusual en una red, generan una alerta y toman medidas correctivas, controlan el acceso y la transmisión de contenido inaceptable u ofensivo.

  Entre su tarea esta:

  - Capacidad automática de reaccionar a los incidentes.
  - Aplicación de nuevos filtros de acuerdo con ataques directos en proceso.
  - Bloqueo automático de ataques efectuados en tiempo real.

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

22.4 Protección del Correo Electrónico (Antispam)

Norma: Se recomienda implementar un sistema, servicio o software para la protección del Correo Electrónico, el cual reducirá la entrada de: mensajes de correo no deseados (spam), enlaces nocivos, programas malignos (malware), contenido engañoso, aplicando políticas en el correo electrónico de la Entidad. Cuando se recibe este tipo de correos electrónicos no deseados, se debe informar al personal de seguridad informática.

Se recomienda difundir las buenas prácticas del uso del correo institucional a los usuarios.

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

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

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

Para evitar ataques de DoS y/o DDoS:

- Se recomienda que los parches y las actualizaciones cuenten con la última versión, distribuir la carga de trabajo en todos los sistemas de servidores y bloquear los paquetes de Protocolo de Mensajería de Control de Internet (ICMP) en accesos externos. Los dispositivos de red utilizan paquetes ICMP para enviar mensajes de error.
- Información o asesoría de los proveedores de servicios de internet (ISP), para asegurarse que las implementaciones estén acorde a la prevención de los ataques de DoS y/o DDoS.
- Implementar un servicio de contingencia para disminuir el impacto de los ataques de DoS y DDoS y que su implementación puede ser local o por nube.

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

22.6 Gestión de Eventos e Información de Seguridad (SIEM)

Norma: Se recomienda la implementación de una Solución SIEM ("*Security Information Event Management*"), la cual es una plataforma 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, recolecta, analiza y priorizan los eventos de seguridad dentro de la red (bitácoras, amenazas, riesgos), y además generan informes de cumplimiento.

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

22.7 Gestión de zona de seguridad

Norma: Se recomienda que exista una "Zona Desmilitarizada" (DMZ) y se configure en los cortafuegos y router, para mantener la seguridad de las redes de confianza de la Entidad.

La zona desmilitarizada es una red aislada que se encuentra dentro de la red interna de la organización. En ella se encuentran ubicados exclusivamente todos los recursos de la entidad que deben ser accesibles desde Internet, como el servidor web o de correo y los servicios DNS. Para el acceso de los servicios de internet se puede implementar las reglas NAT para la seguridad de la red.

SECRETARÍA GENERAL AIG

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

22.8 Protección de Puntos de los Accesos Inalámbricos o Wi-Fi

Norma: Se recomienda contar con una adecuada configuración de los protocolos WPA2 o mayor, para la encriptación de los datos inalámbricos, permisos de acceso, autenticación rigurosa, licenciamiento y monitoreo. El equipo inalámbrico o Wi-Fi debe considerar con las herramientas de protección de los activos de la organización como Control de acceso a la red (NAC) y red privada virtual (VPN), además debe tener sus estándares general IEEE 802.11, con sus protocolos de anticolisiones de banda inalámbrica y autónoma para los canales de 2.4Ghz y 5Ghz, que evite interferencias con otros dispositivos y frecuencias externas.

Se recomienda que los dispositivos en las redes inalámbricas abiertas, públicas e invitados, utilicen túneles VPN (Virtual Private Network) y servicios encriptados para establecer un canal de comunicación seguro en la internet y/o accesos remotos de la Entidad.

Se prohíbe la instalación de puntos de acceso inalámbrico (AP) de uso doméstico dentro de las instalaciones de la Entidad.

Justificación: Evitar la vulnerabilidad inalámbrica de ataques cibernéticos, ayuda en el control e integrada en los dispositivos inalámbricos.

22.9 Protección a la tecnología de Voz sobre IP (VoIP)

Se recomienda que la Entidad que cuenta con una red privada o red segmentada para la telefonía a través del Internet (también llamada "telefonía IP"), o Voice over IP (VoIP), que esta debe ser configurada de forma minuciosa, además de contar con las medidas contra los ataques externos.

Se recomienda consideran los siguientes puntos:

- Debe contar con políticas de calidad de servicio (QoS) en los equipos de enrutamiento para mejorar el rendimiento, la integración y el flujo contra latencias o retardo en la red de voz.
- Implementar reglas o medidas de seguridad con reconocimiento de VoIP en los firewalls.
- Contar con un monitoreo para la transmisión y filtración de señales anormales.
- Añadir servicios proxy como intermediario en las sesiones que solicita el usuario final en sus dispositivos de voz y softphone.
- Diseñar un plan redundante a la red para la disponibilidad de los troncales de voz.
- Cifrar los paquetes de mensajes de voz para protegerlos de las infiltraciones.
- Utilizar el SSH para proteger los gateway y switches.
- Cambiar las contraseñas predeterminadas.
- Utilizar un sistema de detección de intrusiones (IDS) para detectar ataques.
- Utilizar la autenticación sólida para mitigar la suplantación de registros, esto evita que los ciberdelincuentes usurpen o redirigen las llamadas de la Entidad.

22.10 La Seguridad en las Operaciones y Comunicaciones

Norma: El área responsable en la Unidad de TI debe 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 robustecer la seguridad de las comunicaciones y el acceso a la información.

SECRETARÍA GENERAL AIG

23. Software o Malicioso (Malware)

23.1 Prevención proactiva

Norma: Se recomienda establecer un método o control para la verificación de la existencia de "software malicioso", como lo son los virus informáticos, troyanos, gusanos, spyware, adware y ransomware. Los métodos preferidos deberán incluir un enfoque de niveles, mediante mecanismos proactivos y reactivos a través de la red.

Para esta labor, se debe seleccionar herramientas especializadas contra este tipo de software. A la hora de desarrollar estrategias para reducir el malware, es importante definir los puntos clave operativos en que se puede implementar la prevención y/o detección de malware. No dependa únicamente de un sólo dispositivo o tecnología como única línea de defensa.

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

23.2 Antivirus

Norma: Todos los servidores, computadoras y demás dispositivos, deben tener instalados una solución de antivirus, para prevenir, detectar y remover malware (virus, spyware, gusanos, otros), a fin de garantizar el correcto funcionamiento, protección e integridad de los sistemas informáticos.

Se recomienda, que si la cantidad de licencias a administrar es mayor de 50, se utilice una solución de consola de gestión central o un servidor administrativo para los antivirus en los endpoint (accesos a usuario final) para el control, monitoreo, seguridad y actualización de los equipos o dispositivos de comunicación.

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

23.3 Actualizaciones

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

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

24. Buen uso y protección de los equipos de cómputo

24.1 Responsabilidad del funcionario con relación a su equipo asignado

Norma: Para el equipo tecnológico asignado al funcionario, la Unidad de TI o el personal administrativo de la institución (bienes patrimoniales), deben establecer un acta de recibido conforme, en donde se indica las responsabilidades sobre daños o pérdida del equipo.

Los equipos deben ser utilizados estrictamente en tareas relacionadas con su trabajo o función y no para uso personal, en caso de presentarse cualquier problema de software malicioso en su equipo informático, deberán reportarlo inmediatamente a la Unidad de TI.

El funcionario se abstendrá de traer equipo personal, ni efectuar solicitudes a TI de reparaciones o soporte de equipos que no pertenecen a la Entidad, de igual manera el equipo de TI debe de abstenerse de atender este tipo de solicitudes.

Los equipos informáticos que necesiten ser utilizados en actividades fuera de la Entidad, deberán contar con la autorización del Jefe del departamento del funcionario.

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

24.2 Configuración del sistema operativo

Norma: La Unidad de TI de las entidades deberá contar con un manual o lista de verificación en donde se establecen las configuraciones y los aplicativos estándares que se requieran en los equipos según el área o departamento.

De requerir alguna configuración especial o la instalación de otro aplicativo, el funcionario deberá solicitarlo al personal de la Unidad de TI a través de la Mesa de Ayuda de la Entidad. La solicitud deberá estar previamente autorizada y documentada por el supervisor inmediato o encargado de su área de trabajo.

Justificación: Mantener la estandarización en cuanto a la preparación y configuración de los equipos tecnológicos de las entidades.

24.3 Desmontado de equipos

Norma: Ningún funcionario está autorizado para abrir o desmontar los equipos ante algún daño o problema que se muestre. De presentarse una situación como la mencionada, el funcionario debe llamar a los funcionarios de TI de la Mesa de Ayuda para que personal de Soporte Técnico solucione su problema.

Justificación: Prevenir la manipulación de los equipos por personal no autorizado y preservar la garantía de fábrica del equipo donde aplique.

24.4 Almacenamiento de archivos personales

Norma: No es permitido que los funcionarios almacenen archivos 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.

SECRETARÍA GENERAL AIG

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

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

Justificación: Razones de seguridad y de ahorro de energía.

24.6 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.

24.7 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 gestionará 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.

SECRETARÍA GENERAL AIG

25. Control de accesos

25.1 Control de acceso de equipos personales en las redes institucionales

Norma: Se recomienda implementar medidas de seguridad y de control para proteger el acceso a los sistemas y aplicaciones internas por dispositivos personales de los funcionarios. Se debe segmentar la red interna, de las redes de acceso personal (invitado o público) para proteger la información sensitiva de las entidades.

Justificación: Mantener el control de los equipos personales de los usuarios y evitar el acceso no autorizado a la información en la red interna de la Entidad.

25.2 Supervisión y control de sesiones de accesos remotos

Norma: La Unidad de TI deberá asegurar y controlar los accesos remotos mediante la encriptación y el uso de firewalls y redes virtuales seguras (VPN).

Justificación: Mantener supervisión y control de las secciones de acceso remotos en las entidades.

25.3 Controles de accesos y seguridad física en áreas restringidas

Norma: Es recomendable que el área responsable en la Unidad de TI implemente mecanismos de Control y Autenticación en las áreas restringidas dentro de las instalaciones operativas de tecnología para garantizar que solo el personal autorizado tenga acceso

Entre los tipos de Control de Acceso recomendados para las áreas restringidas, se incluyen el Control de Acceso Biométrico con presencia y proximidad, con teclado y reconocimiento facial, entre otros.

Adicional deben mantener un registro de las entradas y salidas de los funcionarios autorizados.

Justificación: Restringir y controlar el acceso a las zonas que contienen equipos que procesen información sensitiva o crítica del Estado y mantener la trazabilidad del acceso de estas zonas.

25.4 Tarjeta de acceso

Norma: Todo funcionario poseedor de una tarjeta de acceso, para el Control de áreas u oficinas de tecnología, tiene la responsabilidad de conservarla en buen estado. Éstas 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: Establecer las responsabilidades de los funcionarios con este mecanismo de control de acceso.

25.5 El Control de Acceso a los Sistemas

Norma: El área responsable en la Unidad de TI debe emplear un procedimiento para la creación de usuarios, asignación de roles y privilegios, identificar los tipos de accesos y derechos en los sistemas.

SECRETARÍA GENERAL AIG

Justificación: Promover la aplicación del control de acceso en los sistemas lo que permite la verificación del acceso a un recurso, a través de un registro histórico de accesos que lo identifique en caso de requerirse.

25.6 Accesos a los Sistemas de Información

Norma: Todos los funcionarios deben tener una identificación única (usuario) y 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.

La responsabilidad de las acciones que un tercero pueda realizar por el uso de la cuenta de un funcionario recae en el funcionario dueño de la cuenta.

Como parte de las mejores prácticas para la creación de contraseñas seguras se recomienda tomar en cuenta los siguientes aspectos:

- 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.

Justificación: Identificar y validar el acceso de los funcionarios a los sistemas por medio de credenciales de forma segura, y restrictiva, para así mantener la seguridad de los sistemas y trazabilidad en los accesos.

25.7 Cambio periódico 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.

Se recomienda que:

- En el proceso de cambio o renovación de las contraseñas, el sistema sea configurado para que no permita reutilizar ninguna de las últimas diez contraseñas.
- Evitar que las contraseñas estén en lugares visibles.
- El funcionario evite anotar su contraseña y dejarla a la vista de otras personas.

Justificación Asegurar la protección de los sistemas y de la información, minimizando el riesgo que las contraseñas puedan ser conocidas por otro usuario y minimizar la vulnerabilidad de acceso a los sistemas por personal no autorizado.

25.8 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 creación de ésta.

Justificación: Garantizar que el funcionario acceda a los sistemas de una forma segura.

25.9 Notificación del vencimiento de contraseñas

Norma: Cuando la contraseña del funcionario esté próxima a expirar, recomendamos que, con 15 días de anticipación, el sistema notifique al usuario de este evento. Esta información debe ser desplegada en pantalla cuando el funcionario inicie sesión.

Todos los funcionarios deben tener presente que sus contraseñas son vulnerables y por ello deben ser cambiadas cada cierto tiempo.

Justificación: Mantener un control del cambio de contraseñas para la seguridad de los accesos a los sistemas.

25.10 Límite de intentos fallidos para acceder al sistema

Norma: Cuando se realiza el proceso de acceso a los sistemas, el límite de intentos fallidos consecutivos debe ser definido en no más de tres (3) intentos; al tercer intento fallido el sistema debe inhabilitar la cuenta del funcionario para acceder al sistema.

El funcionario debe notificar al personal de la Mesa de Ayuda o de la Unidad de TI cuando la cuenta no está activa, para que sea habilitada nuevamente.

Justificación: Robustecer las medidas de seguridad para acceder a los sistemas.

25.11 Contraseñas distintas para cada proceso de autenticación

Norma: Se recomienda que el personal con asignaciones o roles especiales utilicen diferentes 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.

25.12 Bloqueo manual o automático del sistema

Norma: Los funcionarios deben bloquear la computadora antes de dejar su estación de trabajo con el objetivo de no dejar la sesión abierta. Adicionalmente, se debe contar con una política de bloqueo automático para cerrar la sesión del usuario.

Para el buen uso de los sistemas de información sensible el funcionario debe asegurarse cerrar la sesión.

Justificación: Prevenir la utilización indebida de un equipo que tenga una sesión abierta y asegurar la integridad de la información de los datos.

25.13 Doble autenticación

Norma: Se recomienda utilizar la doble autenticación en sistemas críticos de la Entidad que puedan accederse remotamente para aumentar el nivel de seguridad de acceso a los mismos.

Justificación: Asegurar el acceso a los sistemas con la doble autenticación.

25.14 Uso de CAPTCHA

Norma: Se recomienda la utilización de un **CAPTCHA** (Completely Automated Public Turing test to tell Computers and Humans Apart - Test de Turing Público y Automático para distinguir a los ordenadores de los humanos), cuando se requiera asegurar el ingreso solamente por personas, 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.

SECRETARÍA GENERAL AIG

26. Cambios en el control de acceso, por acciones de personal

26.1 Cambio en el control de acceso por Traslados o Reasignación del funcionario

Norma: La Unidad de TI debe coordinar con la Oficina Institucional de Recursos Humanos, para establecer un procedimiento, que será utilizado al momento de producirse el traslado o reasignación de un funcionario y este requiera cambios en el control de acceso. Es preciso implementar un proceso formal del registro y cancelación del usuario en el control de acceso.

Se recomienda aplicar los siguientes lineamientos:

- Informar por escrito al jefe y/o coordinador de la Unidad de TI, el detalle de la nueva posición y/u oficina asignada del funcionario.
- Gestionar la reasignación de las responsabilidades sobre información confidencial y/o reservada que administraba el funcionario.
- Los cambios de posiciones se deberían reflejar en la eliminación de todos los derechos de acceso que no fueron aprobados para el nuevo puesto.

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, como: teléfonos, sistemas de detección, alarmas y control biométrico, tarjetas de accesos, 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.
- Los funcionarios solo deben tener acceso a los servicios que se les ha autorizado específicamente usar.

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

26.2 Retiro de funcionarios

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

- Informar inmediatamente al gerente, director, jefe o coordinador de seguridad de la Unidad de TI, para que se proceda a la revocación de todos los permisos de acceso lógico y físico que posea el individuo, incluyendo el código telefónico, alarmas, suscripciones, fuentes de información, control biométrico, llaves, dispositivos y tarjeta de acceso.
- Se recomienda que cuando un funcionario renuncie o sea desvinculado, los archivos o contenidos almacenados en sus equipos digitales asignados, deben ser examinados por el personal de TI. Se recomienda realizar este procedimiento acompañado de personal de la Oficina Institucional de Recursos Humanos.
- El director de la oficina donde laboraba el funcionario debe designar a un nuevo responsable, en caso de que exista información confidencial y/o privada que necesite ser verificada.

- 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 y mantener la responsabilidad de la custodia de la información confidencial, para conservar las medidas de seguridad mínimas aceptables, previniendo acciones que pueda tomar, en especial, el funcionario destituido o cesado.

26.3 Vacaciones de funcionarios

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

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

26.4 Devolución de equipos del Estado

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

SECRETARÍA GENERAL AIG

27. Accesos y usos del Internet

27.1 Responsabilidad de la entidad en cuanto al servicio de Internet

Norma: Se debe proporcionar un ancho de banda adecuado para el servicio de Internet, voz y datos de la institución. La Unidad de TI debe realizar estudios y la medición del rendimiento de la red, para determinar el ancho de banda adecuado y requerido para el acceso a la Internet con calidad. Dicho estudio deberá quedar documentado.

Justificación: Mantener y establecer un ancho de banda adecuado en pro a la eficiencia y productividad de las operaciones informáticas que se ejecutan en las entidades.

27.2 Responsabilidad del funcionario con relación al uso de Internet

Norma: Todo funcionario con acceso a Internet, debe hacer un buen 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.

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

Norma: Se recomienda implementar medidas de restricción para los funcionarios, que les impida modificar la configuración de sus equipos para navegar por Internet. La configuración de equipos será realizada por personal del área responsable en la Unidad de TI.

Justificación: Controlar la configuración del acceso a Internet.

27.4 Acceso a sitios Web prohibidos y material inadecuado

Norma: Se deben realizar los ajustes para restringir el acceso a sitios Web de contenido adulto o pornográfico, apuestas, juegos de azar, juegos en línea, juegos interactivos, Minería Digital 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.

27.5 Descarga y almacenamiento de material inadecuado

Norma: Se deben tomar medidas para restringir la descarga de programas o material no relacionado con el trabajo o función en los equipos tecnológicos institucionales, y así evitar la entrada de software malicioso: Malwares: Virus, Troyanos, Spywares, Keyloggers, Ransomwares, entre otros.

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

27.6 Sintonización de audio o vídeo a través del Internet

Norma: El jefe de la Unidad de TI debe 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.

SECRETARÍA GENERAL A.I.G

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

27.7 Llamadas a través de Internet

Norma: Las videollamadas a través de internet (Zoom, Microsoft Teams y Google Meet, Webex, entre otros), estará permitido para las labores del funcionario, previamente autorizados por el director o jefe del área responsable donde labora el funcionario; se prohíbe su uso para llamadas personales.

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

SECRETARÍA GENERAL AIG

28. Servicio de correo electrónico institucional

28.1 Uso de plataformas libres para correos electrónicos

Norma: Se recomienda a la Unidad TI, que si van a implementar plataformas libres (OpenSources) de correos electrónicos, éstas deben tener la capacidad de proporcionar confianza en el envío de los datos y compruebe a la Entidad la inexistencia de amenazas potenciales a la privacidad. Algunas plataformas que podemos nombrar son Zimbra, Proton, Zoho Mail, AOL Mail, entre otros.

Justificación: Mantener la confidenciales y la seguridad de la información en los correos electrónicos institucionales.

28.2 Procedimiento de solicitud de correo electrónico

Norma: Toda cuenta de correo electrónico institucional, debe ser solicitado a la Unidad TI por medio de la mesa de ayuda o correo al jefe de la Unidad de TI.

Justificación: Mantener los controles y procedimientos de solicitud de correos electrónicos.

28.3 Cuenta de correo electrónico del funcionario

Norma: Todo funcionario debe utilizar en la red de la institución, una cuenta de correo electrónico de la Entidad (con el dominio institucional) y no de dominios o servicios gratuitos o públicos (Yahoo, Gmail, Outlook.com (antes Hotmail), ProtonMail, iCloud Mail y GMX Mail. entre otros).

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

28.4 Responsabilidad del usuario en el servicio de correo

Norma: Es responsabilidad del funcionario, a partir del momento que se le asigna el buzón de correo electrónico institucional, hacer uso adecuado de la información emitida y recibida, cumpliendo con lo establecido en esta normativa.

Justificación: Responsabilidad del usuario ante las comunicaciones de la Entidad.

28.5 Pie de página de correo electrónico

Norma: La Unidad TI deberá establecer un estándar para el pie de página institucional, llamada usualmente **Firma de correo electrónico.**

Ejemplo del concepto:

- Nombre y Apellido
- Cargo
- Dirección o departamento a que pertenece dentro de la Entidad
- Número de teléfono y correo electrónico
- Imagen o nombre Entidad
- Las cuentas en redes sociales de la Entidad

Es labor de la Unidad TI asegurarse de la disponibilidad, confirmación y conformación de los datos suministrados en la firma del correo electrónico.

Justificación: Asegurar la estandarización e identificación de las firmas oficiales que pertenecen a la Entidad.

28.6 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.

28.7 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 20 MB.

El jefe de la Unidad de TI puede autorizar al personal que requiera el aumento del tamaño de los archivos adjuntos.

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

28.8 Utllizar la cuenta de correo en redes sociales

Norma: Se prohíbe al funcionario utilizar la dirección del correo institucional en Redes Sociales, Comerciales, Foros o cualquier otro sitio que no esté relacionado con la Entidad.

Solo el departamento de relaciones públicas o entes autorizados son los únicos acreditados para compartir correos propagando la difusión de información institucional.

Justificación: Resguardar la información y la integridad de la Entidad.

28.9 Compartir el acceso del correo

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

Justificación: Resguardar la información del Estado.

28.10 Deshabilitar cuentas de Correo Electrónico

Norma: Cuando un funcionario se retire (por renuncia o desvinculación) de la Entidad, el encargado de la oficina de Recursos Humanos debe proceder formalmente enviando un correo electrónico a la Unidad TI (especificando el nombre del funcionario y departamento), para que el personal de seguridad informática tome las siguientes acciones:

- Realizar un respaldo de los correos por funcionario y mantenerlos para futuras consultas.

- . Deshabilitar la cuenta, borrar el buzón de correo (los mensajes permanecen durante 30 días), a menos que se solicite mantener por más tiempo.
- Notificar al jefe inmediato del funcionario que fue deshabilitada la cuenta y que se mantiene una copia de seguridad de ese buzón.

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

28.11 Uso de correo eléctrico en dispositivos móviles personales.

Norma: Evitar en lo posible el uso de cuentas de correos institucionales, en dispositivos móviles personales (laptop, tablets, móviles, etc.).

Justificación: Evitar accesos no autorizados por uso equipos sin la protección adecuada.

SECRETARÍA GENERAL AIG

29. Tecnología Verde

29.1 Establecer estrategias de tecnología verde o ambiental

Norma: Se recomienda que la Unidad de TI implemente el concepto de "Tecnología Verde", en la institución. Éstas se refieren al uso eficiente de los recursos computacionales, minimizando el impacto ambiental, maximizando su viabilidad económica y asegurando deberes sociales. Sobre este punto hablamos de Procesos para el Reciclaje y Gestión de desechos.

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 que 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, teletrabajo, 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.

29.2 Diagnóstico del nivel de implementación de las estrategias

Norma: En el momento que la Unidad de TI decida implementar la Tecnología Verde en la Institución, debe efectuar un diagnóstico para determinar el nivel en que se encuentra la Entidad. 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.

29.3 Actualización de la estrategia

Norma: La estrategia de Tecnología Verde 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.

29.4 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: Como parte de la gestión de estado, ser garantes de la preservación y cuidado ambiental.

29.5 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.

29.6 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.

29.7 Uso eficiente de impresoras

Norma: Se recomienda a la Unidad de TI, la asignación y estandarización de impresora por departamento o dirección, con el objetivo de llevar un control eficiente de las compras y uso de los dispositivos adquiridos, así como el control del inventario de insumos y/o partes.

Justificación: Evitar la compra y uso desmedido de diferentes tipos de impresoras y la disminución de compras de insumos para éstos.

29.8 Implementación de un espacio físico por parte de la Unidad TI

Norma: Se recomienda a la Unidad TI, que los equipos que se encuentran en descarte sean guardados en un espacio físico de almacenamiento, con control de acceso (Biométrico o Clave) antes que se haga el descarte oficial por parte de Contraloría.

Justificación: Preservar el inventario de activos en descarte de la Unidad TI.

29.9 Procedimientos de destrucción de datos y hardware

Norma: Se recomienda a la Unidad TI, la elaboración de métodos o procedimientos aplicables a la eliminación segura de los equipos que se encuentran en descarte (descarte aprobado por Contraloría). Ejemplo de métodos y lineamientos para la destrucción de equipos y datos tecnológicos:

- **Método de desmagnetización de datos:** elimina los datos no solo de la lista de archivos sino de los datos almacenados en el dispositivo, este método es válido para la destrucción de datos de los dispositivos magnéticos, tales como: discos duros, disquetes, cintas magnéticas de respaldo (backup).

SECRETARÍA GENERAL AIG

- **Método de destrucción Física de datos:** método orientado a la destrucción física de los dispositivos de almacenamiento, evitando la recuperación de los datos. El personal asignado que va a destruir los discos duros debe empezar desmantelándonos pieza por pieza, asegurando principalmente la eliminación de la cubierta y platos externos con un objeto punzante para posteriormente realizar el reciclaje físico.
- **Reciclaje de equipo físico:** se recomienda tener un servicio de reciclaje que apoye la destrucción de los equipos computacionales físicos. Entre estos equipos podemos mencionar, tarjetas de circuitos, placas, discos duros, monitores, laptops, CPU, gabinetes de servidores entre otros; siempre y cuando haya sido a aprobado por la contraloría y extraído todos los datos.

Justificación: Utilizar métodos seguros de destrucción de datos, contribuir con el reciclaje de desechos tecnológicos y protección medio ambiente.

30. Consideraciones de servicios de computación en la nube (Cloud) y de alojamiento (Hosting)

30.1 Requisitos para adquisición de servicios en la nube y de alojamiento con terceros

Norma: La Unidad de TI deberá realizar un análisis técnico y de gestión de riesgos, antes de contratar un servicio en la nube o Servicios de Alojamiento de terceros. 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 estos sean requeridos.

Se recomienda contar con personal calificado dentro de la Unidad de TI para los servicios de nube o alojamiento a contratar.

Las condiciones del servicio y obligaciones, tanto del proveedor como del estado, deberán estar contenidas en un contrato formal en conformidad con las regulaciones que apliquen.

Justificación: Identificar y hacer una proyección real de las necesidades de los servicios en la nube. Hay que asegurar que el servicio por contratar cumpla con los requerimientos mínimos y sea verificado por personal idóneo de la Entidad.

30.2 Contrato de prestación de los servicios de nube o de alojamiento

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

- Garantías respecto la privacidad de los datos
- La seguridad y propiedad de los datos
- Controles de acceso y gestión de la información
- Propiedad intelectual de las aplicaciones
- Auditorías
- Administración, manejo, devolución y/o destrucción de los datos al término del contrato
- Tiempo de devolución de los datos al término del contrato

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

30.3 Portabilidad de los datos para los servicios de nube o de alojamiento

Norma: Dentro del contrato de servicio se deberá contemplar una cláusula que indique que el proveedor de servicios garantizará la portabilidad o migración de los datos y servicios (formatos de datos e interfaces de servicios estándar) en caso de finalizar el contrato, así como también deberá establecer de qué manera se va a realizar.

Justificación: Garantizar la seguridad, integridad y disponibilidad de los datos al terminar la relación contractual.

30.4 Restricción de uso para servicios críticos o de seguridad del Estado

Norma: No se deben utilizar servicios de Nube pública como plataformas para alojar servicios de misión crítica o de seguridad del Estado.

SECRETARÍA GENERAL AIG

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

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 con 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.

Se recomienda implementar los principios y guías de los siguientes estándares en su versión vigente:

- ISO/IEC 27032: Gestión de la ciberseguridad
- ISO/IEC 27017: Controles de seguridad para servicios en la nube
- ISO/IEC 27018: Seguridad y protección de información personal en la nube

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

30.6 Disponibilidad de los servicios de nube o de alojamiento

Norma: Se recomienda que el proveedor con el cual se contrate los servicios de Nube o de Alojamiento, cuente con una disponibilidad garantizada de acuerdo con lo definido por el Uptime Institute, los cuales son:

- Tier 2: 99.741% de disponibilidad garantizada
- Tier 3: 99.982% de disponibilidad garantizada
- Tier 4: 99.995% de disponibilidad garantizada

Las instituciones que mantengan contratos con un proveedor que cuenten con el nivel Tier 2, al momento de renovar el servicio, sugerimos considerar integrarse a la Nube Gubernamental de la AIG.

Justificación: Garantizar un alto nivel de confiabilidad, rendimiento y disponibilidad en los centros de datos acorde a los estándares mundiales.

30.7 Versiones del hardware y software que conforman los servicios de nube o de alojamiento

Norma: Se debe asegurar que el hardware y software de los sistemas que conforman los servicios de nube o de alojamiento, cumplan con las versiones más actualizadas para garantizar la continuidad de los servicios adquiridos.

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

SECRETARÍA GENERAL AIG

30.8 Soberanía de Datos.

Norma: Todas las Bases de Datos que contengan información sensitiva de seguridad del Estado o datos institucionales de carácter sensitivo deberán permanecer localizadas en el territorio nacional. A los efectos de esta disposición, se consideran datos o información sensitivas los que califiquen de confidenciales en materia de seguridad nacional, cuya divulgación, alteración o pérdida, pueda comprometer la seguridad del país,

En cuanto a los servicios en la nube de Software como Servicio (SaaS), Plataforma como Servicio (PaaS), Infraestructuras como Servicio (IaaS) y las Bases de Datos, cuya información no esté vinculada a plataformas de seguridad del Estado, como tampoco a los datos institucionales de carácter sensitivo, estos podrán ser contratados por las entidades, para su almacenamiento o custodia fuera del territorio nacional, siempre que medie justificación, a manera de ejemplo: la relación costo beneficio de la contratación.

Se requerirá la evaluación y autorización por parte de la AIG, previo a la realización del procedimiento de contratación.

La solicitud de Autorización deberá incluir la siguiente información:

a) La descripción completa de la información que será alojada.
b) La información del proveedor del servicio que alojará la información.
c) El país en el cual se almacenará la información.
d) El período durante el cual la información será alojada fuera del territorio
e) nacional.
f) Las medidas de seguridad que el proveedor garantiza para la protección de
g) la información.

Recibida la solicitud con la información indicada, se procederá a emitir la autorización, en su defecto, la Autoridad para la Innovación Gubernamental brindará las recomendaciones que deberán ser acatadas para garantizar que los servicios se brindarán bajo parámetros que garanticen la seguridad y protección de los datos.

El almacenamiento o custodia de Bases de Datos que contengan datos personales se regirán por las disposiciones consagradas en la Ley 81 de 26 de marzo de 2019, "Sobre la Protección de Datos Personales".

Justificación: Garantizar la protección del acceso a los datos o información que reposa en las plataformas de seguridad del Estado o datos institucionales de carácter sensitivo.

Contar con un proceso de verificación, control y registro de la información de los servicios en Nube, contratados por las entidades, con almacenamiento o custodia fuera del territorio nacional, en los casos que proceda.

Nota: Referencia Resolución # 42 del 4/10/2024

30.9 Sensibilidad de los datos en servicios en la nube

Norma: Los datos de índole sensibles de la Entidad no deben ser alojados en Nube pública o en alojamiento privado externo. Para estos datos es recomendable su almacenamiento en premisas de la Entidad, tomando en cuenta lo dispuesto anteriormente en este documento de normas.

Se consideran datos sensibles aquellos datos privados de identidad de las personas que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual; así como toda información sobre la seguridad del Estado.

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

30.10 Establecimiento de controles para servicios en la nube

Norma: Se recomienda que los servicios en la nube contratados cuenten con los siguientes controles:

- Monitoreo de tráfico de red y administración de cargas de datos.
- Autentificación multifactor.
- Verificar que los servidores tengan módulos de cifrado por Hardware (HSM, de las siglas en inglés "Hardware Security Module").
- Generación de Informes de condiciones de seguridad de la información (pruebas de vulnerabilidad).

Justificación: Mantener la disponibilidad y estabilidad de los servicios alojados en la nube.

30.11 Alta disponibilidad de los servicios en la nube institucional

Norma: Se recomienda la gestión de dos nubes (híbrida) que se vinculen para la gestión de la carga de trabajo y se mantengan sincronizadas, manteniendo así la alta disponibilidad.

De contar con la redundancia en servicios de nube, la Unidad de TI debe solicitar a los proveedores que realicen las pruebas para verificar que dicha redundancia funcione correctamente y entreguen documentación de los resultados.

Justificación: Asegurar la continuidad de los servicios de la nube institucional.

SECRETARÍA GENERAL AIG

31. Teletrabajo

31.1 Unidad responsable del Teletrabajo

Norma: Se recomienda que el área responsable en la Unidad de TI, implemente y ejecute los mecanismos técnicos y operativos necesarios para el teletrabajo, basado en la Ley 126 de 18 de febrero de 2020 que establece y regula el teletrabajo en la República de Panamá y el Decreto Ejecutivo N° 133 del 16 de septiembre de 2020 que reglamenta la Ley de Teletrabajo y dicta otra disposición.

Justificación: Establecer el alcance, roles y responsabilidades para la implementación de herramientas tecnológicas para el teletrabajo en las entidades; basándose en el marco legal.

31.2 Recursos informáticos para el Teletrabajo

Norma: La Unidad de TI revisará los requisitos y recursos de infraestructura, software, ancho de banda y licenciamientos necesarios para la ejecución del teletrabajo y operaciones informáticas.

Justificación: Garantizar la disponibilidad y conectividad a los sistemas de la Entidad en cumplimiento del ejercicio de teletrabajo.

31.3 Controles en el Teletrabajo

Norma: La Unidad de TI deberá establecer los procedimientos y controles para la preparación de los equipos tecnológicos permitidos para el desarrollo de las funciones en la modalidad de teletrabajo. Además, se deberá realizar una definición del trabajo permitido e informar los horarios correspondientes, la clasificación de la información, los sistemas y servicios internos a los que el teletrabajador estará autorizado a acceder, así como también, establecer los elementos de auditoría, monitoreo y control de seguridad, en coordinación con la oficina institucional de Recursos Humanos.

Justificación: Definir los parámetros de gestión interna sobre los procedimientos y controles que se deberán llevar a cabo en los equipos tecnológicos para el desarrollo de las funciones de teletrabajo.

31.4 Seguridad en el Teletrabajo

Norma: Establecer las medidas necesarias para mantener la seguridad física y digital, respecto a la confidencialidad de la información. El equipo no deberá ser prestado ni utilizado por terceros y debe mantenerse bloqueado en todo momento cuando no se esté utilizando. Para estos casos se recomienda que todo equipo de cómputo que esté en modalidad de teletrabajo se deberá cifrar o encriptar las unidades de almacenamiento y de igual manera se deberá verificar el bloqueo de puertos USB mientras estén en la modalidad de teletrabajo.

Justificación: Definir los parámetros de seguridad para protección de la información en la modalidad de teletrabajo.

31.5 Soporte en el Teletrabajo

Norma: Se recomienda que la Unidad de TI establezca las directrices y procedimientos para el suministro de soporte en cuanto a hardware y software de los equipos usados para el teletrabajo.

Justificación: Definir los parámetros al soporte remoto de los equipos tecnológicos.

32. GLOSARIO

Considere las siguientes definiciones de uso, al presente documento.

1. **ACL (Lista de Control de Acceso):** es un conjunto de reglas para el filtrado del tráfico o paquetes, que controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete.
2. **Activos de Información**: son elementos considerados de interés para los objetivos de la Entidad. Son los recursos necesarios para que una Entidad funcione.
   - Datos
   - Software
   - Hardware y redes de comunicación
   - Sistemas y aplicaciones de informática
   - Servicios contratados
3. **ADC (Controlador de Entrega de Aplicaciones):** es un dispositivo de red que gestiona las conexiones de cliente hacia aplicaciones complejas web y empresariales.
4. **Administrador de Seguridad Informática:** Gestiona la seguridad de los sistemas informáticos y de telecomunicaciones.
5. **Agenda Digital Nacional (ADN):** es el informe quinquenal con las principales líneas de acción, metas y programas prioritarios y relevantes para la modernización del estado, con el objetivo disminuir la brecha de la desigualdad, aumentar la competitividad y la capacidad de resiliencia de las entidades públicas. Pretende ser una Guía de la Innovación Gubernamental y su impacto en la sociedad, para permitir conocer mejor las innovaciones globales y como Panamá las está adoptando; su efecto en la ciudades, comunidades, ciudadanos y empresas,
6. **Alta Disponibilidad - High Availability (HA):** Se refiere a la habilidad de un sistema de operar continuamente sin fallar por un designado periodo de tiempo. Un sistema de alta disponibilidad trabaja para garantizar que un sistema cumpla con un nivel de rendimiento operativo acordado.
7. **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.
8. **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.

9. **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.
10. **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.
11. **BIA (Análisis de Impacto al Negocio):** es un proceso sistemático para determinar y evaluar los efectos potenciales de una interrupción de las operaciones críticas como resultado de un desastre, accidente o emergencia.
12. **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.
13. **Cableado Estructurado:** sistema de cables, conectores, y dispositivos que permiten establecer una infraestructura de telecomunicaciones informáticas en un edificio.
14. **Calidad de Servicio (QoS):** es la descripción o medida del rendimiento promedio que se espera en una conexión de red, para así asegurar la priorización de tráfico y la garantía de ancho de banda.
15. **CAPTCHA:** es un acrónimo de (Completely Automated Public Turing test to tell Computers and Humans Apart) Test automático y Público para diferenciar humanos de computadoras y consiste en una prueba para comprobar si el usuario es un humano y no un robot y así evitar que algún software de spam acceda a un sitio web.
16. **Cloud:** del inglés "Cloud Computing", y conocida también como: servicios en la Nube, Informática en la Nube o Nube Computacional, y es un esquema que permite ofrecer servicios de computación o recursos o almacenaje a demanda en servidores virtuales a través de una red, que usualmente es 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).
17. **Confianza Cero (Zero Trust):** es un método de ciberseguridad basado en la creencia de que las organizaciones no deben confiar automáticamente en nada, ya sea fuera o dentro del perímetro de su red. Los modelos de confianza cero exigen que todo lo que intente conectarse a los sistemas de una organización debe verificarse para que se le conceda acceso.
18. **Configuración:** conjunto de datos que determina el valor de algunas variables de un programa, dispositivo o de un sistema operativo.

19. **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.
20. **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.
21. **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.
22. **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.
23. **DMZ (Zona Desmilitarizada):** es una red aislada del resto de la red interna, donde se ubican únicamente los servidores que deben ser accesibles desde Internet.
24. **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.
25. **EDR (Detección y Respuesta de Punto Final)** acrónimo en inglés de Endpoint Detection Response: es un sistema de protección de los equipos e infraestructuras de la entidad Combina el antivirus tradicional junto con herramientas de monitorización e inteligencia artificial para ofrecer una respuesta rápida y eficiente ante los riesgos y las amenazas más complejas.
26. **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.
27. **Encriptación:** codificación de la información (archivos, correo electrónico), para protegerla frente a terceros, mientras la información viaja por la red.
28. **Entidad:** toda colectividad que puede considerarse como una unidad, en especial, cualquier corporación, compañía y Entidad, etc.
29. **Equipo Servidor:** es un equipo informático que forma parte de una red y provee servicios a otros equipos clientes.
30. **ETL (Extracción, Transformación y Carga):** es un método de integración de los datos que no están optimizados que consiste en extraer, transformar y cargar múltiples fuentes

de información para almacenarlas en un solo destino o almacén de datos que simplifica su gestión y análisis.

31. **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.
32. **Gateway (puerta de enlace):** es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más ordenadores.
33. **Hardware:** conjunto de elementos físicos que constituyen una computadora o un sistema informático.
34. **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.
35. **Interoperabilidad:** como la habilidad de dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada.
36. **Jefe de la Unidad de TI:** Gerente, director, jefe o persona a cargo de la Unidad de TI en la Entidad.
37. **Keylogger:** es un tipo de software malicioso que registra todas las pulsaciones de teclas que realice el usuario en el ordenador.
38. **Licencia de software:** las licencias de software son un contrato entre el autor de un programa informático y los usuarios de este. En ellas se establecen los términos, condiciones y cláusulas que se deben cumplir para poder usar ese programa y cada usuario que se descarga, instala, copia o lo utiliza debe aceptar esas condiciones.
39. **Malware:** es un término que se utiliza para describir el software diseñado para interrumpir las operaciones de la computadora u obtener acceso a los sistemas informáticos, sin el conocimiento o el permiso del usuario.
40. **Máxima Autoridad de la Entidad:** es la dependencia administrativa de más alta posición, en la jerarquía de la estructura organizacional de la Entidad.
41. **NAC (Control de Acceso a la Red):** también llamado Control de Admisión a la Red, es un método para reforzar la seguridad, la visibilidad y la gestión de acceso de una red propietaria. Restringe la disponibilidad de los recursos de la red a los dispositivos finales y usuarios que cumplen con una política de seguridad definida.
42. **NAT (Traductor de Direcciones de Red):** permite que redes de computadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten al Internet usando una única dirección IP (IP pública).

43. **NDR (Detección y Respuesta de Red):** están diseñadas para detectar amenazas cibernéticas en infraestructura de redes mediante el aprendizaje automático y el análisis de datos.
44. **Norma:** regla que se debe seguir o a la que se deben ajustar las conductas, tareas, actividades, etc.
45. **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.
46. **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.
47. **Plan de simplificación de trámites:** este plan debe contener los proyectos destinados a mejorar la relación con los ciudadanos y empresas, la reducción de burocracia y mejora de productividad mediante la reducción de procedimientos, costos, requisitos y tiempo de los trámites administrativos con el fin de brindar un servicio ágil y eficiente, utilizando para ello cualquier medio que le facilite el trámite al usuario.
48. **Plan Operativo Anual (POA):** es el plan de los proyectos presupuestados y aprobados en la Agenda Digital (ADN), todas las instituciones deben presentarlo el último trimestre de cada año.
49. **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.
50. **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.
51. **Protocolo de Mensajería de Control de Internet (ICMP):** protocolo para enviar mensajes de error, como un servicio solicitado que no está disponible o un host que no puede llegar a un router.
52. **Proxy:** es un sistema que sirve de intermediario en las peticiones de los recursos que realiza el cliente a servidores.
53. **Ransomware:** es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos y en donde el "hacker" exige el pago de un rescate para poder devolver el acceso al sistema o datos.
54. **Recuperación de Desastre - Disaster recovery (DR):** Se refiere a las actividades que requieren para realizar la restauración de una base de datos, en el evento de una interrupción técnica o evento catastrófico (E.g. corte de energía, fuego, inundación, vandalismo, ataque cibernético u otros).

SECRETARÍA GENERAL AIG

55. **RPO (Punto Objetivo de Recuperación):** volumen de datos (expresado en tiempo) en riesgo de pérdida que la organización considera tolerable. Es decir, determina el objetivo de posible pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema.

56. **RTO (Tiempo Objetivo de Recuperación):** expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus sistemas y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

57. **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.

58. **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.

59. **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.

60. **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.

61. **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.

62. **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.

63. **Sistema Operativo:** conjunto de programas de un sistema informático que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas.
64. **Softphone:** es una aplicación de software que se instala en un dispositivo conectado a Internet y que permite realizar llamadas telefónicas.
65. **Software:** conjunto de programas y rutinas que permiten a los dispositivos realizar determinadas tareas.
66. **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.
67. **Software libre:** software cuyo código fuente puede ser estudiado, modificado, y utilizado libremente con cualquier finalidad y redistribuido con cambios o mejoras sobre ellas.
68. **Spam:** correos no deseados que se envían de forma masiva por Internet o mediante otros sistemas de mensajería electrónica.
69. **Spyware:** es un software que permite a un delincuente obtener información de un usuario y sus actividades informáticas dentro de un computador.
70. **SSH (Shell Seguro):** es un protocolo que proporciona una conexión de administración segura (cifrada) a un dispositivo remoto.
71. **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.
72. **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.
73. **Trámite en Línea:** es un trámite realizado mediante el uso de las TIC en relación con 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.
74. **Troyanos:** es un malware que ejecuta operaciones maliciosas bajo la apariencia de una operación deseada. Este código malicioso ataca los privilegios de usuario que lo ejecutan.
75. **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.
76. **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.
77. **VPN (Red Privada Virtual):** es un canal virtual seguro que utiliza la red pública (es decir, Internet) y permite establecer una conexión protegida utilizando redes públicas. Las VPN

SECRETARÍA GENERAL AIG

cifran su tráfico en internet y disfrazan su identidad en línea. Esto le dificulta a terceros el seguimiento de sus actividades en línea y el robo de datos. El cifrado se hace en tiempo real.

78. **WPA2 (Wi-Fi Protected Access 2):** (Acceso protegido Wi-Fi 2) es un protocolo cifrado de seguridad que protege el tráfico de Internet en redes inalámbricas. La segunda generación del protocolo de seguridad de Acceso protegido Wi-Fi (WPA2) aborda errores anteriores y ofrece un cifrado más potente.

79. **XDR (Detección y Respuesta Extendidas):** es un sistema que tiene la opción de detectar amenazas y dar respuesta a incidencias de seguridad, vinculando automáticamente datos de varias fuentes, que pueden incluir los puntos finales o endpoint, redes y usuarios.

SECRETARÍA GENERAL AIG