SUPLEMENTO

REGISTRO OFICIAL
ÓRGANO DE LA REPÚBLICA DEL ECUADOR

SUMARIO:

Págs.

Año III - Nº 583 - 64 páginas
Quito, martes 23 de noviembre de 2021

RESOLUCIÓN No. 157-SO-12-CACES-2021

El Consejo de Aseguramiento de la Calidad de la Educación Superior

Considerando:

Que, el artículo 353 de la Constitución de la República del Ecuador determina: "El Sistema de Educación Superior se regirá por: (…) 2. Un organismo público técnico de acreditación y aseguramiento de la calidad de instituciones, carreras y programas, que no podrá conformarse por representantes de las instituciones objeto de regulación.";

Que, el 12 de octubre de 2010 entró en vigor la Ley Orgánica de Educación Superior - LOES, norma que fue modificada a través de la Ley Orgánica Reformatoria a la LOES, publicada el 02 de agosto de 2018, en el Suplemento del Registro Oficial Nro. 297, de cuyo contenido se colige que el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES) es el Organismo al que hace referencia el numeral 2 del artículo 353 de la Constitución de la República;

Que, el artículo 171 de la Ley ibidem determina que el Consejo de Aseguramiento de la Calidad de la Educación Superior es: "(…) el organismo público técnico, con personería jurídica y patrimonio propio, con independencia administrativa, financiera y operativa que tiene a su cargo la regulación, planificación y coordinación del sistema de aseguramiento de la calidad de la educación superior; tendrá facultad regulatoria y de gestión (…)";

Que, mediante Acuerdo Ministerial No. 025-2019 de 20 de septiembre de 2019, publicado en el Registro Oficial Edición Especial No. 228 de 10 de enero de 2020, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) acordó: "Art. 1.- Expedir el Esquema Gubernamental de Seguridad de la Información -EGSI-, el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, que se encuentra como Anexo al presente Acuerdo Ministerial.";

Que, el artículo 6, literal a) del Acuerdo Ministerial No. 025-2019 señala que el Comité de Seguridad de la Información tendrá, entre otras responsabilidades, la de gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución;

Que, mediante Resolución Nro. 029-P-CACES-2020, de 14 de mayo de 2020, reformada mediante Resolución Nro. 035-P-CACES-2020, de 04 de junio de 2020, el presidente de este Consejo resolvió designar al Comité de Seguridad de la Información institucional, que se conforma por los siguientes servidores: "1. Director/a Administrativo Financiero/a; 2. Coordinador/a General Técnico/a; 3. Director/a de Estudios e Investigaciones; 4. Director/a de Evaluación y Acreditación de Universidades y Escuelas Politécnicas; 5. Director/a de Evaluación y Acreditación de Institutos Superiores; 6. Director/a de Aseguramiento de la Calidad; 7. Director/a de Talento Humano; Jefe/a de la Unidad de Planificación; 8. Jefe/a de la Unidad de Comunicación Social; 9. Responsable de la Unidad de Tecnologías de la Información; y, 10. Coordinador/a General de Asesoría Jurídica, que participará en calidad de asesor";

Que, mediante Resolución Nro. 078-SE-22-CACES-2020, de 03 de agosto de 2020, el Pleno de este Organismo resolvió: "(…) Expedir la Política de Seguridad de la Información en el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES), la cual se adjunta y forma parte integrante de la presente Resolución";

Que, conforme Acta de reunión de trabajo Nro. 14 del Comité de Seguridad de La Información (CSI), de 06 de julio de 2021, se aprobó la propuesta plan de auditoría al EGSI V2.0. con observaciones;

Que, mediante Documento Nro. GDE-UPGE-POL-01, de 06 de julio de 2021, suscrito por el ingeniero Wilman Patricio Vivanco Jiménez, Oficial de Seguridad de la Información de este Organismo se pone en conocimiento de este Consejo el proyecto de "política de Seguridad de la Información en el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES), el mismo que es aprobado conforme lo indicado en el considerando que antecede;

Que, mediante sumilla electrónica inserta a través del Sistema de Gestión Documental Quipux, en el Memorando Nro. CACES-CSI-2021-0039-M, de 31 de agosto de2021, el Econ. Juan Manuel García Samaniego, Presidente de este Consejo dispuso: "(…) Aprobado: trámite pertinente conforme a normativa vigente, elaborar la resolución correspondiente para conocimiento y aprobación del Pleno";

Que, mediante Memorando CACES-PR-2021-0381-M de 01 de octubre de 2021 el Abg. Luis Carrera, remitió a la Presidenta del CACES el Informe de sustento y el proyecto de resolución respecto de la Política de Seguridad de la Información en el Consejo de Aseguramiento de la Calidad de la Educación Superior;

Que, mediante sumilla inserta el 14 de octubre de 2021, a través del Sistema de Gestión Documental Quipux, en el Memorando citado, la Presidenta del CACES dispuso incluir en el orden del día de la sesión del pleno de este Consejo el punto referido en el considerando que antecede y el proyecto de resolución respectivo; y,

En ejercicio de las atribuciones que le confiere la Ley Orgánica de Educación Superior, el Acuerdo Ministerial No. 025-2019, y demás normativa pertinente,

RESUELVE:

Artículo 1.- Expedir la Política de Seguridad de la Información en el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES), la cual se adjunta en documento Nro. GDE-UPGE-POL-01, de 06 de julio de 2021 y forma parte integrante de la presente Resolución.

Artículo 2.- Encárguese de la ejecución de la Política de Seguridad de la Información en el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES) a la Coordinación General Administrativa Financiera, Procuraduría, Secretaría Técnica, Direcciones y Unidades del CACES en el campo de las atribuciones asignadas en la política citada.

Artículo 3.- Encárguese del seguimiento a la ejecución de la presente Resolución al Comité de Seguridad de la Información.

Artículo 4.- Encárguese a la Unidad de Comunicación la difusión de la Política de Seguridad de la Información entre los servidores institucionales, en función del Plan de Comunicación y Sensibilización del EGSI versión 2.0, que para el efecto desarrolle.

DISPOSICIONES GENERALES

Primera. - Notifíquese la presente Resolución al Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), ente rector encargado del seguimiento al cumplimiento obligatorio de la Política de Seguridad.

Segunda. - Notifíquese la presente Resolución al Oficial de Seguridad de la Información, a los miembros del Comité de Seguridad de la Información Institucional, Coordinación General Administrativa Financiera, Procuraduría, Secretaría Técnica y Unidades del CACES.

DISPOSICIÓN DEROGATORIA

Única: Deróguese la Resolución Nro. 078-SE-22-CACES-2020, de 03 de agosto de 2020, y todo acto administrativo contrario a la presente Resolución.

DISPOSICIÓN FINAL

La presente Resolución entrará en vigencia a partir de la fecha de su expedición.

Dada en la ciudad de San Francisco de Quito, D.M., en la Décima Segunda Sesión Ordinaria del pleno del Consejo de Aseguramiento de la Calidad de la Educación Superior, llevada a cabo a los veintiún (21) días del mes de octubre de 2021.

Firmado electrónicamente por:
WENDY AMERICA ANZULES FALCONES

Dra. Wendy Anzules Falcones
PRESIDENTA DEL CACES

En mi calidad de Secretaria del pleno del CACES (E.F), **CERTIFICO** que la presente Resolución fue discutida y aprobada por el pleno del Consejo de Aseguramiento de la Calidad de la Educación Superior, en su Décima Segunda Sesión Ordinaria, llevada a cabo a los 21 días del mes de octubre de 2021.

Lo certifico.-

Firmado electrónicamente por:
DANIELA ALEJANDRA AMPUDIA VITERI

Ab. Daniela Ampudia Viteri
SECRETARIA DEL PLENO DEL CACES (E.F)

CACES
Consejo de Aseguramiento de la Calidad de la Educación Superior

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN EL CONSEJO DE ASEGURAMIENTO DE LA CALIDAD DE LA EDUCACIÓN SUPERIOR

(CACES)

2021

Código:	GDE-UPGE-POL-01
Fecha de emisión:	06/07/2021

Rubro	Nombre y Cargo	Firma	Fecha
APROBADO POR:	**Pleno del Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES)**		
REVISADO POR:	Comité de Seguridad de la Información	Acta Nro. 14 del Comité de Seguridad de la Información	06/07/2021
ELABORADO POR:	Wilman Patricio Vivanco Jiménez **Oficial de Seguridad de la Información**	Firmado electrónicamente por: WILMAN PATRICIO VIVANCO JIMENEZ	06/07/2021

NIVEL DE CONFIDENCIALIDAD	Baja
NIVEL DE INTEGRIDAD	Baja
NIVEL DE DISPONIBILIDAD	Baja

Registro de Cambios en el Documento			
Versión	**Descripción de la Modificación**	**Aprobado por (Nombre y Cargo)**	**Fecha**
1.0	Creación	Alex Batallas Presidente del Comité de Seguridad de la Información	15/06/2020
2.0	Modificación de denominaciones de Unidades de Gestión en la Política de Seguridad de la Información y modificación de denominaciones de jefes a responsables.	Alex Batallas Presidente del Comité de Seguridad de la Información	06/07/2021

CONTENIDO

1. Declaración de la Política de Seguridad de la Información

Es responsabilidad del CACES, y compromiso con la ciudadanía, garantizar la legitimidad, objetividad, imparcialidad y transparencia de los procesos de aseguramiento de la calidad de la educación superior, mediante la adopción de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001, que permita minimizar los riesgos y prevenir eventos e incidentes de seguridad que atenten contra la integridad, disponibilidad y confidencialidad de la información interna y externa usada para el cumplimiento de los objetivos de este Consejo.

2. Objetivos de la Política

Los objetivos de la Política de Seguridad de la Información son:

- Proteger, resguardar y asegurar la disponibilidad, integridad, confidencialidad, legalidad y confiabilidad de los activos de información y tecnologías para su procesamiento.
- Identificar, clasificar y tratar los riesgos de seguridad de la información.
- Minimizar los riesgos de seguridad de la información de los procesos clave de la institución.
- Identificar, clasificar, categorizar y mantener actualizados los activos de información.
- Determinar los roles, responsabilidades y competencias de los servidores públicos que tengan relación con los activos de información.
- Establecer las directrices, procedimientos e instructivos relacionados con la seguridad de la información.
- Monitorear la implementación del Sistema de Gestión de la Información, estableciendo mecanismos de seguimiento y control de los activos de información y tecnologías de procesamiento.
- Difundir la Política de Seguridad de la Información y capacitar a todos los servidores públicos del CACES.

3. Alcance y usuarios

La Política de Seguridad de la Información aplica para todas las personas sean

naturales o jurídicas que tengan algún tipo de relación jurídica, laboral o contractual con el CACES y que procesen, almacenen o transfieran información de la institución o entregada a la institución para su manejo y custodia, en cualquier forma, impresa, digital o verbal, tanto de manera temporal como permanente, dentro y fuera de la institución.

4. Revisión de la Política para la Seguridad de la información

Para garantizar la vigencia de la política de seguridad de la información, esta debe ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económico, entre otros; los cuales deben ser documentados y versionados.

5. Política Global de Seguridad de la Información

La Política Global de Seguridad de la Información del CACES incluye pautas específicas que serán una guía para el manejo adecuado de la información de la institución y responder por la integridad, confidencialidad y la disponibilidad. Estos aspectos de seguridad de la información se fundamentan en los dominios y objetivos de control de la "Guía para la implementación de controles de seguridad de la información (NTE-INEN ISO/IEC 27002:2017), que se encuentra en los anexos del Acuerdo Ministerial No. 25, publicado en el Registro Oficial Edición Especial 228 de 10 de enero de 2020.

Estas políticas guiarán el comportamiento personal y profesional de todas las personas sean naturales o jurídicas que tengan algún tipo de relación jurídica, laboral o contractual con el CACES, sobre la información obtenida, generada o procesada por la institución; de igual manera las políticas permitirán que la institución trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales está obligada a cumplir.

Las políticas serán revisadas por el Comité de Seguridad de la Información y aprobadas por el presidente del CACES.

5.1. Organización de la seguridad de la información

Establecer lineamientos para administrar la seguridad de la información dentro del Consejo de Aseguramiento de la Calidad de la Educación Superior y establecer un marco de gestión para controlar su implementación y operación.

5.1.1. Organización interna

5.1.1.1. Roles y responsabilidades en seguridad de la información

Para cumplir los objetivos de la Política de Seguridad de la Información del CACES se establecen los siguientes roles y responsabilidades:

Pleno del CACES

- Responsables de aprobar la Política y sus futuras modificaciones con la asesoría del Comité de Seguridad de la Información (CSI) del CACES.

Presidente del Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES):

- Designar al interior la institución, un Comité de Seguridad de la Información (CSI), de conformidad con las directrices del Ministerio de Telecomunicaciones y de la Sociedad de la Información, órgano rector encargado de desarrollar y coordinar planes, programas, o proyectos sobre gobierno electrónico.
- Gestionar los recursos necesarios para la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en función de la proforma anual presupuestaria aprobada por el pleno del CACES.

Comité de Seguridad de la Información (CSI):

- El Comité de Seguridad de la Información cumplirá con las responsabilidades establecidas por el Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información y, las demás responsabilidades que demanden las necesidades institucionales para la implementación del EGSI o referentes a la seguridad de la información, dispuestas por el presidente del CACES o el pleno del CACES.

Oficial de Seguridad de la Información (OSI)

- El Oficial de Seguridad de la Información cumplirá con las responsabilidades establecidas por el Ministerio encargado del sector de las

Telecomunicaciones y de la Sociedad de la Información y, las demás responsabilidades que demanden las necesidades institucionales para la implementación del EGSI o referentes a la seguridad de la información, dispuestas por el presidente del CACES o el pleno del CACES.

Servidores Públicos del Nivel Jerárquico Superior (NJS) y Responsables de las Unidades de Gestión

- Responsables de garantizar que los servidores públicos que trabajan bajo su control protejan la información de acuerdo con las normas establecidas en este documento y las requeridas por las necesidades institucionales como protocolos y procedimientos específicos correspondientes a la seguridad de la información.

Servidores públicos del CACES

- Cumplir con la Política de Seguridad de la Información y mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

5.1.1.2. Separación de tareas

Para la separación de las tareas se debe contar con los procesos definidos y documentados; así como un manual de funciones que sea de conocimiento del personal del CACES. Esto para que al asignar las responsabilidades el personal conozca los roles que tiene dentro de la institución.

Es responsabilidad de los servidores públicos del CACES conocer la estructura organizacional y los procesos de su dirección, para distinguir dónde parten sus funciones y responsabilidades y dónde comienzan las funciones de sus compañeros de área o proceso. De igual manera, los servidores públicos deben conocer el nivel de confidencialidad de la información que manejan.

La Dirección de Administración del Talento Humano velará porque el recurso humano incorporado a la institución cuente con el perfil necesario para desempeñar con responsabilidad y calidad las labores encomendadas.

Toda la documentación formal debe pasar por tres etapas como:

- Elaboración.
- Revisión.
- Aprobación.

Ningún servidor está facultado para realizar por sí mismo todas etapas de validación de documentación, así como la custodia.

5.1.1.3. Contacto con las autoridades

Todo incidente de seguridad de la información que sea considerado crítico deberá ser reportado al Oficial de Seguridad de la Información, este a su vez debe informar al Comité de Seguridad de la Información y remitir al presidente para que conforme con el Reglamento Interno del CACES presente al Pleno del Consejo para su conocimiento y resolución.

La Unidad de Tecnologías de la Información y Comunicaciones deberá identificar y mantener actualizados los datos de contacto de proveedores de bienes o servicios de telecomunicaciones o de acceso a Internet para gestionar potenciales incidentes.

5.1.1.4. Contacto con grupos de interés especial

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, el presidente del CACES, el Oficial de Seguridad de la Información y/o el servidor delegado en la institución, podrán mantener contacto con cualquier otra institución pública o privada con la que se necesite mantener relaciones de cooperación para efectos del cumplimiento de la presente política. Además, estas comunicaciones deben reportarse al presidente del CACES. Como ejemplo de los contactos con grupos de interés se tiene los siguientes:

- Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL).
- Corporación Nacional de Telecomunicaciones CNT EP
- Dirección Nacional de Registros de Datos Públicos.
- Instituciones de Educación Superior.

En los intercambios de información de seguridad, no se divulgará información confidencial ni información pública a cargo del CACES sin la autorización

correspondiente. El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permite cuando se tenga la autorización del presidente del CACES y cuando se haya firmado un Acuerdo de Confidencialidad previo o con aquellas Organizaciones especializadas en temas relativos a la seguridad informática y cuyo personal esté obligado a mantener la confidencialidad de los temas que tratan. El Comité de Seguridad de la Información será el responsable de mantener actualizada esta información.

5.1.1.5. Seguridad de la información en la gestión de proyectos

Independientemente de la naturaleza del proyecto en el CACES debe considerarse la seguridad de la información.

En los proyectos que se planifiquen se debe: considerar los objetivos de seguridad en los objetivos del proyecto, determinar los riesgos de seguridad de la información para identificar e implementar los controles necesarios y en todas las fases de la metodología aplicada en el proyecto incluir la seguridad de la información.

En los documentos, tales como contratos o convenios o cualquier instrumento legal, la Procuraduría deberá velar por la inclusión de cláusulas de protección de la información.

5.1.1.6. Seguridad cuando se trata con ciudadanos o usuarios

El servidor responsable de facilitar servicios a ciudadanos o usuarios de instituciones públicas o privadas deberá primero identificar requisitos mínimos de seguridad, en el caso de que se utilice o procese información de la institución o de estos. Se debe, al menos, considerar los siguientes criterios:

- Protección de activos de información.
- Descripción del producto o servicio.
- Las diversas razones, requisitos y beneficios del acceso del usuario.
- Política de control del acceso.
- Descripción de cada servicio que va a estar disponible.
- Nivel de servicio comprometido y los niveles inaceptables de servicio.
- El derecho a monitorear y revocar cualquier actividad relacionada con los Activos de la institución;
- Las respectivas responsabilidades civiles de la institución y del usuario;
- Las responsabilidades relacionadas con asuntos legales y la forma en que se

garantiza el cumplimiento de los requisitos legales.

- Derechos de propiedad intelectual y asignación de derechos de copia y la protección de cualquier trabajo colaborativo.
- Protección de datos con base en la Constitución y leyes nacionales, particularmente datos personales o financieros de los ciudadanos.

5.1.2. Las computadoras portátiles y el teletrabajo

5.1.2.1. Política de uso de computadoras portátiles

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar una política de uso de computadoras portátiles, que deberá ser socializada e implementada.

Es responsabilidad de los servidores públicos del CACES proteger los equipos que se le han asignado para el desempeño de sus funciones, así como mantener la seguridad de la información que se genere, siguiendo como mínimo, las medidas que a continuación se describen:

- No exponer el equipo a condiciones de inseguridad física y/o ambiental.
- Proteger las claves de acceso que le han sido asignadas.
- Proteger la información que se almacene en el dispositivo móvil hasta que se genere un respaldo de la documentación en el computador de la institución asignada al servidor o hasta que se entregue esa información al servidor designado para custodia.

Las computadoras portátiles personales, no otorgadas por el CACES, que requieran acceso a los servicios de la institución, deben contar con la validación de la Unidad de Tecnologías de la Información y Comunicaciones, de que cuentan con los elementos tecnológicos de seguridad informática.

Para las computadoras portátiles de propiedad del CACES, la Unidad de Tecnologías de la Información y Comunicaciones deberá:

- Restringir la instalación de software.
- Restricciones de conexión a sistemas de gestión de la información, excepto en aquellos casos que se tiene una autorización por parte del presidente del CACES justificando la necesidad de acceso.

- Manejar y reportar los controles de acceso.
- Mantener la protección contra virus.
- Control sobre la utilización de servicios y aplicaciones web.
- Generar respaldos en casos de cambio de equipos o cambios administrativos de servidores públicos.

5.1.2.2. Teletrabajo

La Dirección de Administración del Talento Humano y la Unidad de Tecnologías de la Información y Comunicaciones deben elaborar una política de teletrabajo y medidas de seguridad de apoyo, para proteger la información a la que se accede, procesa o almacena en ubicaciones destinadas a esta modalidad de trabajo. Esta política debe ser socializada e implementada.
Los servidores públicos del CACES que laboren en modalidad de teletrabajo deben cumplir con las siguientes medidas de seguridad:

- Minimizar la amenaza de un intento de acceso no autorizado a la información o a los recursos por parte de otras personas de la misma ubicación, por ejemplo, familia y amigos.
- Mantener el computador o equipo móvil actualizado para prevenir ataques informáticos a sus dispositivos.
- Guardar la información que se genere en la nube o en los sistemas de gestión documental proporcionados por la institución, previo a un acceso autorizado.
- Recopilar toda la información que se realice como parte del trabajo en una sola carpeta en el computador o el equipo móvil hasta que se pueda generar un respaldo y ser entregado a la Unidad de Tecnologías de la Información y Comunicaciones al finalizar su relación laboral con el CACES.
- Cambiar la clave de red inalámbrica utilizando una clave de alta seguridad para mejorar el nivel de seguridad.
- Evitar abrir correos maliciosos que pongan en riesgo el equipo y la información que se almacena.
- Recibir soporte remoto por parte de la Unidad de Tecnologías de la Información y Comunicaciones del CACES.

5.2. Seguridad de los recursos humanos

Establecer criterios para asegurarse que los servidores públicos y las personas sean naturales o jurídicas que tengan algún tipo de relación jurídica, laboral o contractual con el CACES sean idóneos para las funciones para las que han sido requeridos y comprendan sus responsabilidades.

5.2.1. Antes del empleo

5.2.1.1. Investigación de perfil de competencias

La Dirección de Administración del Talento Humano llevará a cabo controles de verificación para asegurar que el perfil de competencias del candidato sea el más adecuado para cumplir con el puesto requerido. Para tal efecto, se debe realizar la comprobación del perfil de competencias de los candidatos, contratistas o usuarios de terceras partes, designaciones y promociones de servidores públicos de acuerdo con los reglamentos, la ética y las leyes pertinentes.

5.2.1.2. Términos y condiciones del empleo

Todos los servidores públicos y las personas sean naturales o jurídicas que tengan algún tipo de relación jurídica, laboral o contractual con el CACES, como parte de sus obligaciones contractuales, deberán firmar un acuerdo de confidencialidad que proteja la información obtenida voluntaria o involuntariamente, según el ámbito de su competencia y los niveles de acceso a la información que posea.

Los acuerdos de confidencialidad serán elaborados y actualizados por Procuraduría y aprobado por el presidente del CACES o su delegado.

La copia firmada del Acuerdo deberá ser retenida en forma segura por la Dirección de Administración del Talento Humano.

Para la firma del Acuerdo de Confidencialidad se debe considerar:

- Suscripción inicial del acuerdo de confidencialidad por parte de la totalidad de los servidores públicos.
- Método de re-suscripción en caso de modificación del texto del Acuerdo de Confidencialidad.

5.2.2. Durante el empleo

5.2.2.1. Responsabilidades de gestión

Es responsabilidad de la Dirección de Administración del Talento Humano gestionar la suscripción e inducción a las personas naturales o jurídicas que tengan algún tipo de relación jurídica, laboral o contractual con el CACES sobre la existencia de la Política de Seguridad de la Información y promover su cumplimiento.

Es responsabilidad de los mandos medios y superiores de las áreas, difundir y hacer cumplir a todo personal a su cargo la Política de Seguridad de la Información.

5.2.2.2. Concienciación, educación y capacitación en seguridad de la información

Es responsabilidad del servidor público NJS, promover en todo momento, la participación en los procesos de concientización, capacitación y prevención a incidentes de seguridad, a todo el personal a su cargo, para fortalecer una cultura de seguridad de la información.

La Dirección Administración del Talento Humano deberá incluir como parte de la inducción al personal de nuevo ingreso y a las personas que sean naturales o jurídicas que tengan algún tipo de relación jurídica, laboral o contractual con el CACES, el material informativo necesario sobre seguridad de la información.

El Oficial de Seguridad de la Información a través del Comité de Seguridad de la Información debe establecer programas orientados a fortalecer y afianzar una cultura de seguridad de la información en el personal de la Institución.

La Unidad de Comunicación Social es la encargada de elaborar el Plan de Comunicación y Sensibilización del EGSI, que incluye la difusión de la Política de Seguridad de la información a todos los servidores públicos del CACES.

5.2.2.3. Proceso disciplinario

En caso de incumplimiento de las disposiciones de la presente política, normas y procedimientos de seguridad del CACES, los infractores serán sancionados de conformidad a su gravedad, de acuerdo con las normas que rigen al personal del CACES y la normativa vigente en el ámbito de aplicación de la LOSEP, del Código de Trabajo y demás normativa en el ámbito administrativo, civil y penal conforme corresponda.

5.2.3. Finalización del empleo o cambio en el puesto de trabajo

5.2.3.1. Responsabilidades ante la finalización o cambio

Toda terminación laboral, debe apegarse a los procesos involucrados de la Dirección de Administración de Talento Humano, Coordinación General Administrativa Financiera y de la Unidad de Tecnologías de la Información y Comunicaciones, promoviendo que la separación del puesto sea de una manera ordenada, disminuyendo así el riesgo hacia los activos de información que son propiedad de la institución.

Los servidores públicos NJS son los responsables de comunicar de forma inmediata y oportuna a la Dirección de Administración de Talento Humano, a la Coordinación General Administrativa Financiera y a la Unidad de Tecnologías de la Información y Comunicaciones, sobre la finalización del nombramiento, contrato o cambio de puesto de los servidores públicos o de las personas que sean naturales o jurídicas que tengan algún tipo de relación jurídica, laboral o contractual con el CACES.

Todos los servidores públicos o personas que sean naturales o jurídicas que tengan algún tipo de relación jurídica, laboral o contractual con el CACES, previa la terminación de un contrato deberán realizar la transferencia de la documentación e información de la que fue responsable al nuevo servidor a cargo, en caso de ausencia, al servidor público del nivel jerárquico superior o responsable de unidad, al Oficial de Seguridad de la Información y al responsable designado de la Unidad de Tecnologías de la Información y Comunicaciones. De igual manera, se deberá entregar al responsable designado de la Coordinación General Administrativa Financiera, el equipo informático y mobiliario propiedad del CACES en buenas condiciones tal como fue entregado.

5.3. Gestión de activos

5.3.1. Responsabilidad de los activos

5.3.1.1. Inventario de activos

Un activo de información es un elemento reconocible que almacena datos, registros, información en cualquier medio y que tiene las características siguientes:

- Es valioso para el CACES por la información que contiene.
- No es de fácil reemplazo y en algunos casos pudiera ser irrepetible.

Es responsabilidad de los servidores públicos del nivel jerárquico superior y responsables de unidad identificar sus activos de información. Se debe mantener un inventario de los archivos generados por los servidores públicos, tanto de manera física como electrónica, razón de ser de la función que desempeñan en la institución. Los servidores públicos deben reportar y entregar la información a los servidores públicos del nivel jerárquico superior y responsables de unidad a la que pertenecen.

La Unidad de Tecnologías de la Información y Comunicaciones, debe mantener un registro actualizado sobre los activos informáticos que soporten los servicios TIC del CACES, esto es soporte de Hardware y soporte de Software.

5.3.1.2. Propiedad de los activos

Todos los activos que figuran en el inventario deben tener asignado un responsable y autorizado por el servidor público del nivel jerárquico superior o responsable de unidad.

El servidor público responsable del activo debe:

- Salvaguardar la integridad, disponibilidad y confidencialidad del activo.
- Asegurar que los activos son clasificados y protegidos debidamente.
- Hacer uso del activo únicamente para los propósitos y actividades de la institución.
- Reportar al servidor público del nivel jerárquico superior o responsable de unidad y este a su vez al Oficial de Seguridad de la Información de cualquier incidente, problema o vulnerabilidad relacionado con el activo de información.
- Realizar lo necesario para mantener el activo de información en buenas condiciones que garantice y cumpla su función.
- Asegurar el manejo adecuado para el borrado o destrucción del activo.

5.3.1.3. Uso aceptable de los activos

El CACES considera que los recursos para el procesamiento de la información son prioritarios para el desarrollo de los procesos de la institución y el adecuado cumplimiento de sus funciones; por lo que, es responsabilidad de los servidores públicos el salvaguardar de cualquier alteración o modificación no autorizada, daño o destrucción que limite su disponibilidad para el adecuado desarrollo de sus actividades.

El uso aceptable de los activos de información incluye:

- La información y documentos generados en la institución y enviados por cualquier medio o herramienta electrónica son propiedad de la misma institución.
- El correo electrónico institucional debe utilizarse exclusivamente para las tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
- Cada servidor es responsable tanto del contenido del mensaje enviado como de cualquier otra información que adjunte.
- Los servidores públicos son responsables por la destrucción de los mensajes con origen desconocido, y asume la responsabilidad por las consecuencias que pueda ocasionar la ejecución de los archivos adjuntos.
- Para el envío y la conservación de la información, debe implementarse el cifrado (criptografía) de datos.
- Los servidores públicos deberán notificar de cualquier necesidad de protección o mejora, en los controles para los activos de información.

La Unidad de Tecnologías de la Información y Comunicaciones será la responsable de elaborar, socializar e implementar una política de acceso a internet. De igual manera son los responsables de manejar los accesos y uso de la internet y sus aplicaciones/servicios; para esto, se debe considerar las responsabilidades y roles de los servidores públicos. La Unidad de Tecnologías de la Información y Comunicaciones debe limitar el acceso a los servidores públicos a portales, aplicaciones o servicios del internet y la web que pudieren perjudicar los intereses y la reputación de la institución o que atenten a la ética y moral.

5.3.1.4. Devolución de activos

Todo personal que preste sus servicios al CACES, al concluir sus funciones, debe cumplir con lo que se establece en este documento en el apartado “6.2.3.1. Finalización o cambio de empleo” y tiene la obligación de entregar los activos informáticos asignados en buen estado físico y de operación, así como los activos de información y la documentación correspondiente.

5.3.2. Clasificación de la información

5.3.2.1. Directrices de Clasificación de la información

Todos los servidores públicos que sean responsables de algún activo de información deben clasificar la información en relación con su valor, normativa legal vigente, sensibilidad y criticidad para la institución y/o el estado, ante revelación o modificación no autorizada.

La clasificación de los activos de información se la debe realizar considerando los tres pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad.

La información según el nivel de confidencialidad debe clasificarse como:

Pública (baja): toda información en cualquier formato que puede ser conocida y utilizada sin autorización por cualquier persona, sea servidor del CACES o no.
Interna (media): información que puede ser conocida y utilizada por un grupo de servidores públicos, que la necesiten para realizar su trabajo, y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves al CACES o terceros.
Confidencial (alta): aquella información que no está sujeta al principio de publicidad y comprende aquella que sólo puede ser conocida y utilizada por un grupo de servidores públicos que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar afectaciones significativas al CACES o a terceros.

La información según el nivel de integridad debe clasificarse como:

- Baja: información cuya modificación no autorizada, si no es detectada, no afecta la operación del CACES.
- Media: información cuya modificación no autorizada, si no es detectada, podría ocasionar pérdidas significativas para el CACES o terceros.
- Alta: información cuya modificación no autorizada, si no es detectada, podría ocasionar pérdidas graves al CACES o a terceros.

La información según el nivel de disponibilidad debe clasificarse como:

- Baja: información cuya inaccesibilidad no afecta las operaciones del CACES.
- Media: información cuya inaccesibilidad podría ocasionar pérdidas significativas para el CACES o terceros.
- Alta: información cuya inaccesibilidad podría ocasionar pérdidas graves para el

CACES o terceros.

-

5.3.2.2. Etiquetado de la información

La Unidad de Planificación y Gestión Estratégica, responsable de la administración por procesos del CACES, establecerá los procedimientos para el rotulado, tanto en formatos físicos como electrónicos, teniendo en cuenta por lo menos las siguientes pautas generales:

- Se etiquetarán todos los activos de Información conforme con el esquema de clasificación de información: confidencialidad, integridad y disponibilidad.
- Para toda la documentación que se elabore en el CACES se colocará el nivel de confidencialidad: baja, media, alta.
- Incluir datos mediante abreviaturas, acerca del tipo de activo y su funcionalidad para la generación de etiquetas.
- En caso de repetirse la etiqueta del activo, deberá añadirse un número secuencial único al final.
- Las etiquetas generadas deberán estar incluidas en el inventario, asociadas a su respectivo activo. La Unidad de Documentación y Archivo tomará en cuenta que en los inventarios documentales se contemple el etiquetado.
- Los responsables de los activos supervisarán el cumplimiento del proceso de generación de rotulación de los activos.
- En caso de destrucción de un activo, la etiqueta asociada a éste debe mantenerse en el inventario respectivo con los registros de las acciones realizadas.

5.3.2.3. Manejo de los activos

Los responsables de los activos de información deben considerar lo siguiente:

- Restringir el acceso a la información de acuerdo con su clasificación, definiendo usuarios autorizados a los activos.
- Todo activo de información protegido según su clasificación debe contar con un control de acceso, donde se establezca qué personas son las autorizadas para el manejo de la información en el activo
- Los servidores públicos están obligados a no revelar a terceras personas la información que conozcan por el ejercicio de sus funciones, por lo que están obligados a mantenerla confidencial y privada para evitar su divulgación.

- Los usuarios de acuerdo con sus funciones podrán trabajar y hacer uso de la información institucional en los activos de información asignados y resguardar la versión final.

5.3.3. Manejo de los soportes de almacenamiento - medios

5.3.3.1. Gestión de medios extraíbles

La Unidad de Tecnologías de la Información y Comunicaciones, debe proporcionar los servicios necesarios para asegurar el manejo de la información dentro del CACES.

Para la gestión de medios extraíbles se debe considerar:

- Cuando sea necesario por la norma legal vigente de la institución, solicitar la autorización para extraer medios de la institución, debiendo mantener el registro respectivo para mantener la trazabilidad por efectos de auditoría.
- Todos los medios deberían almacenarse en un entorno seguro y protegido, conforme a las especificaciones de sus fabricantes.
- Deben emplearse técnicas criptográficas para proteger datos en medios extraíbles en caso de que apliquen requisitos importantes de confidencialidad o integridad.
- Los datos deberían transferirse a medios de fabricación reciente antes de que se conviertan en ilegibles, a fin de modificar el riesgo de degradación del medio durante el tiempo en que los datos almacenados aún son necesarios.
- Deben almacenarse copias múltiples de datos valiosos en medios separados para reducir aún más el riesgo de daño o pérdida simultánea de los datos.
- El registro de medios extraíbles debería considerarse para limitar las posibilidades de pérdida de datos.

5.3.3.2. Eliminación de los medios

Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios, mediante procedimientos formales. La Unidad de Tecnologías de la Información y Comunicaciones debe establecer procedimientos para asegurar la baja y el borrado confiable de los activos informáticos, así como establecer procedimientos para identificar los elementos que requieran una eliminación segura.

La eliminación de elementos sensibles debe quedar registrado a fin de mantener trazabilidad para su auditoría.

5.3.3.3. Transferencia de medios físicos

Durante el transporte fuera de los límites físicos del CACES, los medios que contengan información deberían estar protegidos contra accesos no autorizados, usos indebidos o deterioro, considerando la criticidad de la información; para lo cual se debe:

- Emplearse un servicio fiable de transporte o mensajería.
- Embalar de forma segura medios o información enviada a través de servicios de mensajería.
- Mantenerse registros e identificar el contenido de los medios, la protección aplicada, así como reflejar los momentos de transferencia a los custodios y la recepción en el destino.

5.4. Control de acceso

5.4.1. Requisitos institucionales para el control de acceso

5.4.1.1. Política de control de acceso

La Unidad de Tecnologías de la Información y Comunicaciones debe definir la política para el acceso a la información, considerando quien tiene la necesidad de conocer los niveles de seguridad, considerando la clasificación de la información. En esta política se debe establecer, al menos, los siguientes aspectos:

- Definir responsabilidades para identificar, gestionar y mantener perfiles de los custodios de información.
- Los requisitos para la autorización formal de los pedidos de acceso.
- Procedimiento de gestión de los accesos de los usuarios a los sistemas de información asegurando el acceso de usuarios autorizados y previniendo los accesos no autorizados.
- Definir claramente los autorizadores de los permisos de acceso a la información.
- Considerar quien tiene la necesidad de conocer la información y los niveles de seguridad, considerando la clasificación de la información.
- Considerar la norma legal vigente sobre el acceso a datos o servicios.

5.4.1.2. Acceso a redes y servicios de red

La política de control de accesos en cuanto al acceso a redes y servicios de red debe contener los siguientes criterios:

- Permitir identificar a los usuarios autorizados para acceder a las redes y servicios de red a través de VPN, redes virtuales y redes inalámbricas entre otras;
- Establecer procedimientos de autorización que determinen quiénes tienen permitido el acceso a qué redes y a qué servicios de red.
- Establecer los controles necesarios para el ingreso a la red y los procedimientos respectivos para proteger el acceso a las conexiones de red y a los servicios de la red.

Para controlar el acceso a redes y servicios de red la Unidad de Tecnologías de la Información y Comunicaciones debe:

- Documentar los equipos que se encuentran en las redes debidamente autorizados.
- Monitorear que el equipo esté con relación a la autenticación del usuario.
- Monitorear el uso de los servicios de la red, con alertas sobre aquellos recursos que se considere críticos.

5.4.2. Gestión de acceso de los usuarios

5.4.2.1. Registro y retiro de usuarios

Para el registro y retiro de usuarios que haga posible la asignación de los derechos de acceso, la Unidad de Tecnologías de la Información y Comunicaciones debe:

- Crear los accesos para los usuarios, verificando previamente que exista la solicitud por parte del servidor público del nivel jerárquico superior o jefe de unidad y que se haya firmado el acuerdo de confidencialidad.
- Proporcionar accesos temporales a usuarios externos o terceros de acuerdo con el tiempo de su permanencia y limitados según las actividades para las que fueron contratados; para esto se debe verificar previamente que exista una solicitud del servidor público del nivel jerárquico superior o jefe de unidad y que se haya firmado el acuerdo de confidencialidad.
- Modificar y eliminar los accesos de los usuarios, solo si se cuenta con la solicitud del servidor público del nivel jerárquico superior o responsable de unidad.

- Suspender temporalmente los accesos de los usuarios en caso de vacaciones, comisiones, licencias, es decir, permisos temporales. Para tal efecto, la Dirección de Administración de Talento Humano deberá notificar si existe este tipo de cambios en los servidores públicos. Esta suspensión temporal de los accesos será para los sistemas en los cuales se maneje información sensible.
- Mantener un registro de la gestión de accesos a aplicaciones, redes, que evidencie, fecha de creación, eliminación, suspensión, activación o eliminación del acceso; al igual que de cada usuario, disponer de los permisos de acceso que han sido asignados.

5.4.2.2. Provisión de acceso a usuarios

Todos los accesos a servicios de tecnologías de la información y aplicativos deben ser asignados de acuerdo con su función, mediante roles y perfiles, propiciando una correcta segregación de funciones.

5.4.2.3. Gestión de los derechos de acceso con privilegios especiales

Los usuarios con privilegios especiales de acceso deben contar con la autorización del responsable del activo o del servidor público del nivel jerárquico superior o responsable de unidad. Las cuentas de usuarios con privilegios especiales de acceso deben ser diferentes a las cuentas que utilizan para la operación.

5.4.2.4. Gestión de la información confidencial de autenticación de los usuarios

La Unidad de Tecnologías de la Información y Comunicaciones debe asegurar la confidencialidad de la entrega de contraseñas en todos sus procesos.

5.4.2.5. Revisión de los derechos de acceso de usuario

Los propietarios de los activos deberán revisar o coordinar la revisión de los derechos de acceso, a intervalos regulares definidos por la institución.

5.4.2.6. Retiro o adaptación de los derechos de acceso

Es responsabilidad de la Dirección de Administración de Talento Humano, notificar las bajas o cambios de adscripción de los servidores públicos a la Unidad de Tecnologías de la Información y Comunicaciones, para la ejecución del cambio o remoción de los derechos de acceso.

Es responsabilidad de los servidores públicos del nivel jerárquico superior o responsables de unidad que cuenten con personal externo, que tengan acceso a los servicios de tecnología de la información y a los aplicativos Institucionales, notificar las bajas o cambios de funciones del personal a la Unidad de Tecnologías de la Información y Comunicaciones, para la ejecución del cambio o remoción de los derechos de acceso.

5.4.3. Responsabilidades del usuario

5.4.3.1. Uso de la información confidencial para la autenticación

Todos los servidores públicos del CACES son responsables de su contraseña, para lo cual deben cumplir con los siguientes criterios de seguridad:

- La contraseña es confidencial, debe mantenerse secreta y se debe asegurar su no divulgación, incluyendo a personas con autoridad.
- Evitar guardar (por ejemplo, en papel, en un fichero software o en un dispositivo portátil) las credenciales de acceso, a no ser que esta pueda ser almacenada de forma segura y que el método de almacenamiento haya sido aprobado (por ejemplo, en repositorios seguros para contraseñas).
- Cambiar las contraseñas siempre que haya indicios de su posible divulgación o vulneración.
- Cambiar la contraseña inicial, después de que le fue asignada al sistema o aplicativo, empleando contraseñas de calidad que sean fáciles de recordar.

5.4.4. Control de acceso a sistemas y aplicaciones

5.4.4.1. Restricción del acceso a la información

La Unidad de Tecnologías de la Información y Comunicaciones debe asegurar que las aplicaciones cuenten con un control de acceso centralizado, donde el usuario debe ser identificado con un user-id y una contraseña segura. Además, deben implementar controles sobre los perfiles de acceso de los usuarios, por ejemplo, de lectura, de escritura, de borrado y de ejecución de la información, etc.

Todos los usuarios con acceso a los aplicativos institucionales deben identificarse en forma única y contar con los derechos de acceso asignados previamente, de acuerdo con su rol y perfil.

5.4.4.2. Procedimientos seguros de inicio de sesión

La Unidad de Tecnologías de la Información y Comunicaciones debe verificar que todo aplicativo institucional cuente con las configuraciones necesarias para limitar el tiempo de la sesión activa. Además, deben limitar la cantidad de intentos permitidos de registro de inicio de sesión, máximo tres intentos; así como deben llevar un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema, generando la alerta respectiva.

5.4.4.3. Sistema de gestión de contraseñas

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar, socializar e implementar la política para la gestión de contraseñas, que permita contar con un control de contraseñas seguro y un mecanismo de historial, para evitar la no reutilización de estas.

5.4.4.4. Uso de herramientas de administración de sistemas

La Unidad de Tecnologías de la Información y Comunicaciones debe restringir y controlar estrictamente el uso de herramientas que puedan estar en capacidad de anular los controles del mismo sistema.

5.4.4.5. Control de acceso al código fuente del programa

La Unidad de Tecnologías de la Información y Comunicaciones debe contar con un mecanismo para controlar el acceso a la consulta del código fuente de los sistemas o aplicativos de la Institución.

5.5. Criptografía

5.5.1. Controles criptográficos

5.5.1.1. Política de uso de los controles criptográficos

La Unidad de Tecnologías de la Información y Comunicaciones debe establecer una política que será revisada por el Comité de Seguridad de la Información, que regule el uso de controles criptográficos y claves para la protección de la información.

La Unidad de Tecnologías de la Información y Comunicaciones debe utilizar los controles criptográficos en los siguientes casos, estableciendo los algoritmos de cifrado para los distintos escenarios:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada como confidencial.
- Para el resguardo de información, cuando así surja de la evaluación de riesgos.

5.5.1.2. Gestión de claves

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar una política para la gestión de claves. También, se deberá implementar procedimientos para generar claves para los diferentes sistemas criptográficos y diferentes aplicaciones; así como para almacenar claves, incluyendo la forma de acceso a las mismas, por parte de los usuarios autorizados.

5.6. Seguridad física y del entorno

5.6.1. Áreas seguras

5.6.1.1. Perímetro de seguridad física

La Coordinación General Administrativa y Financiera debe informar al Comité de Seguridad de la Información la designación de las áreas seguras de la institución.

La Coordinación General Administrativa y Financiera y la Unidad de Tecnologías de la Información y Comunicaciones conforme con sus atribuciones, son las responsables de definir un espacio físico seguro, que cumpla con lo mínimo para asegurar el procesamiento y almacenamiento de la información, para lo cual se deberá considerar, al menos, lo siguiente:

- Todas las puertas del perímetro de seguridad deben estar dotadas de un sistema de alarma, monitorizadas y probadas juntamente con las paredes, para establecer el nivel requerido de resistencia de acuerdo con las normas regionales, nacionales e internacionales; se debería operar de acuerdo con los códigos locales de protección contra incendios en modo de fallo seguro.
- Se debe implementar los mecanismos necesarios que permitan limitar el acceso a las áreas seguras, solamente para el personal autorizado.
- Disponer de alarmas de incendio y puertas de evacuación debidamente monitoreadas que cumplan normas nacionales e internacionales.
- Disponer de un sistema de vigilancia mediante el uso de circuitos cerrados de televisión.

- Controlar el acceso físico, se deben restringir los accesos a las instalaciones del CACES, únicamente al personal autorizado.

5.6.1.2. Controles físicos de entrada

Las áreas seguras deben estar protegidas mediante controles de ingreso adecuados, para asegurar que únicamente se permita el acceso al personal autorizado.

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por la Coordinación General Administrativa y Financiera. Estos controles de acceso serán, por lo menos, los siguientes:

- Supervisar la permanencia de los visitantes en las áreas restringidas y registrar la hora y fecha de su ingreso y salida, sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
- Controlar y limitar el acceso, exclusivamente a personal autorizado, a la información clasificada y a las instalaciones de procesamiento de información.
- Mantener y monitorear de manera segura un libro físico de registro o una pista de auditoría electrónica de todos los accesos.
- Implementar el uso de una identificación visible para todo el personal y visitantes, quienes deberán ser escoltados por una persona autorizada para el tránsito en las áreas restringidas.
- Para el personal proveniente de terceras partes que prestan servicios de soporte, proporcionar acceso restringido a las áreas seguras o a las instalaciones de procesamiento de la información confidencial únicamente cuando sea requerido; este acceso debería estar autorizado y controlado.
- Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas. Se utilizarán controles de autenticación para autorizar y validar todos los accesos. Se mantendrá un registro protegido para permitir auditar todos los accesos.

5.6.1.3. Seguridad de oficinas, despachos e instalaciones

La Coordinación General Administrativa y Financiera debe proporcionar a cada empleado un espacio físico asignado que cuente con mobiliario protegido para el resguardo de información física.

Además, se debe proporcionar a cada empleado un acceso controlado para el uso de las instalaciones de acuerdo con sus funciones dentro del CACES. El acceso a áreas restringidas debe ser autorizado por el servidor público del nivel jerárquico superior o responsable de unidad.

5.6.1.4. Protección contra las amenazas externas y ambientales

La Coordinación General Administrativa y Financiera debe establecer controles para la protección física contra desastres naturales, ataques maliciosos o accidentes. Dentro de estos controles deben constar, al menos, los siguientes:

- Ubicar los equipos de repuesto y soporte a una distancia prudente para evitar daños en caso de desastre que afecte las instalaciones principales.
- Suministrar el equipo apropiado contra incendios y ubicarlo adecuadamente.
- Realizar mantenimientos de las instalaciones eléctricas y UPS.
- Adoptar controles para minimizar el riesgo de amenazas físicas potenciales como robo, incendio, explosión, humo, agua, polvo, vibración, efectos químicos, interferencia del suministro eléctrico e interferencia a las comunicaciones, entre otros.
- Trabajo en áreas seguras.

5.6.1.5. Trabajo en áreas seguras

El acceso a las áreas seguras o a las instalaciones de procesamiento de la información confidencial del CACES, deben ser controladas y debe restringirse el acceso no autorizado. En estas áreas no está permitido los equipos de grabación, cámaras, equipos de video y audio, computadoras portátiles, etc., a menos de que estén autorizados por el servidor público del nivel jerárquico superior o jefe de unidad.

5.6.2. Seguridad de los equipos

5.6.2.1. Ubicación y protección de equipos

La Coordinación General Administrativa y Financiera deberá establecer controles para la protección de los equipos, para minimizar el riesgo de posibles amenazas físicas y ambientales y de oportunidades de acceso no autorizado.

5.6.2.2. Instalaciones de suministro

Las instalaciones de procesamiento de información que opera el CACES deben contar con equipos que suministren energía eléctrica de forma ininterrumpida por al menos 24 horas, tales como generadores y UPS. Estos generadores deben contar con procedimientos documentados de mantenimiento y uso.

5.6.2.3. Seguridad del cableado

El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información debe estar protegido frente a interceptaciones, interferencias o daños. Para lo cual se debe, al menos, manejar los siguientes controles:

- No debe estar expuesto a condiciones ambientales que aceleren su deterioro, tales como: agua, corrosivos, exceso de calor, etc.
- Todo el cableado de datos debe estar debidamente etiquetado en los paneles de parcheo y adecuadamente instalado, para facilitar su mantenimiento.
- Cuando exista un cambio en el cableado, se debe actualizar la memoria técnica correspondiente.
- El cableado de datos y de energía debe estar separado en distintitas canaletas o ductos, para evitar interferencias, siguiendo las normas aplicables.
- El acceso a los cuartos donde residan los paneles de parcheo y tableros de distribución eléctrica, deben ser restringido al personal responsable de la red y del soporte técnico o mantenimiento de esta.

5.6.2.4. Mantenimiento de los equipos

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar, socializar, implementar, evaluar y mantener registros del plan de mantenimiento que garantice la disponibilidad e integridad continua de los equipos.

5.6.2.5. Salida de los activos fuera de las instalaciones de la institución

La Coordinación General Administrativa Financiera debe elaborar un protocolo con los controles de seguridad para la salida e ingreso de equipos de las instalaciones del CACES, considerando la normativa legal vigente.

5.6.2.6. Seguridad de los equipos y activos fuera de las instalaciones

La Coordinación General Administrativa Financiera debe elaborar un protocolo con los controles de seguridad que se debe seguir para los equipos que se encuentren fuera de

las instalaciones del CACES (domicilio personal, teletrabajo y lugares de trabajo temporales), considerando los riesgos que surgen al trabajar fuera de las mismas.

5.6.2.7. Seguridad en la reutilización o eliminación segura de dispositivos de almacenamiento

La Unidad de Tecnologías de la Información y Comunicaciones, debe contar con un protocolo que incluya las técnicas de seguridad para la destrucción, borrados o sobrescribir los dispositivos que contienen información sensible, los cuales no permitan la recuperación de la información original, antes de su retirada o reutilización de estos dispositivos.

5.6.2.8. Equipo informático de usuario desatendido

La Unidad de Tecnologías de la Información y Comunicaciones, debe implementar en todo equipo informático las configuraciones necesarias para su bloqueo de forma automática en un tiempo máximo de 5 minutos, una vez que éste se encuentre desatendido.

5.6.2.9. Política de puesto de trabajo despejado y pantalla limpia

Todos los servidores públicos que presten sus servicios dentro de las instalaciones del CACES deben cumplir con los siguientes lineamientos al ausentarse de su estación de trabajo o al finalizar su jornada laboral:

- Mantener bajo llave la información sensible (cajones o archiveros), en especial cuando no estén en uso y no se encuentre personal en la oficina.
- Retirar del escritorio cualquier tipo de información sensible sin importar el medio en que se encuentre (papel, post-it, discos, medios magnéticos) y resguardarla en los cajones, archiveros o cualquier otro mueble con acceso controlado (llave).
- Las claves es una información sensible que no debe estar en los escritorios ni en las pantallas.
- Destruir de manera segura aquella información que ya no será utilizada.
- No dejar documentos con información, principalmente sensible, sobre impresoras, copiadoras, etc.
- No utilizar la información impresa que sea confidencial o de uso restringido para reciclaje.

5.7. Seguridad de las operaciones

5.7.1. Procedimientos y responsabilidades operacionales

5.7.1.1. Documentación de procedimientos de operación

La Unidad de Tecnologías de la Información y Comunicaciones es responsable de documentar sus procedimientos y contar con memorias técnicas para la administración de los aplicativos y sistemas de información, mismos que deben estar actualizados y vigentes. Estos procedimientos corresponden, por lo menos, los siguientes:

- Procedimiento en la instalación y configuración de sistemas.
- Procesamiento y manejo de la información tanto automatizada como manual.
- Proceso de respaldo y restauración de la información.
- Procesos de los servicios de procesamiento de datos, incluyendo la interrelación con otros sistemas.
- Procedimiento para el manejo de errores y otras condiciones excepcionales que pueden surgir durante la ejecución de las tareas incluyendo restricciones en las funcionalidades del sistema.
- Procedimientos de las instrucciones para el manejo de los medios de resultados especiales, como el uso de papel especial o la gestión de resultados confidenciales, incluyendo procedimientos de eliminación segura de resultados producidos como consecuencia de tareas fallidas.
- Procedimientos para reinicio y recuperación del sistema en caso de fallas.
- Procedimientos de monitoreo de los sistemas.

5.7.1.2. Gestión de cambios

La Unidad de Tecnologías de la Información y Comunicaciones debe establecer un proceso documentado para la gestión de cambios en los ambientes operativos.

Todo servidor que participe en un cambio, en un componente de algún servicio TIC o sus elementos de configuración, deben apegarse estrictamente a los lineamientos establecidos en el proceso “Gestión de cambios”.

5.7.1.3. Gestión de capacidades

La Unidad de Tecnologías de la Información y Comunicaciones debe monitorear el uso de los recursos y proyectar los requerimientos de capacidad a futuro de acuerdo con la gestión institucional, con el fin de analizar las tendencias para el desempeño de los sistemas y aplicaciones.

5.7.1.4. Separación de ambientes de desarrollo, pruebas y producción

La Unidad de Tecnologías de la Información y Comunicaciones debe mantener separados los ambientes de producción, prueba y desarrollo, para reducir riesgos de acceso no autorizado o cambios al sistema; considerando el establecimiento de reglas para el desarrollo o mantenimiento de software y su implementación en producción.

Los ambientes de desarrollo y de producción deben ubicarse en segmentos diferentes. Los ambientes de prueba deben ser lo más parecido posible, en todos los aspectos, al ambiente de producción buscando así implementaciones efectivas.

La Unidad de Tecnologías de la Información y Comunicaciones debe establecer mecanismos para la protección de datos e información sensible o reservada. Los compiladores, editores y servicios relacionados con el desarrollo de sistemas no deben ser accesibles en el ambiente de producción.

5.7.2. Protección contra un software malicioso

5.7.2.1. Controles contra software malicioso

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar una política formal para prohibir el uso de software no autorizado por la institución, que incluya un listado del software autorizado. Esta política debe ser socializada a los servidores públicos del CACES, considerando también información puntual sobre software malicioso y los controles de seguridad que se debe ejecutar.

La Unidad de Tecnologías de la Información y Comunicaciones debe asegurar que todos los equipos de escritorio, móviles (laptops) y servidores utilizados en la red del CACES, tengan instalado el software antivirus, anti-malware, anti-xploits, anti-spam y anti-spyware institucional y mantenerlo actualizado, tanto en versión como en definición de firmas. Así mismo, deben cumplir con una configuración base de parches de seguridad.

5.7.3. Copias de seguridad

5.7.3.1. Copias de seguridad de la información

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar, implementar y socializar la política de copias de seguridad de la información, verificando periódicamente su validez.

Todos los servidores públicos del nivel jerárquico superior o jefes de unidad son responsables de identificar la información que sea sensible para la operación de su área de acuerdo con su criticidad y deben notificar a la Unidad de Tecnologías de la Información y Comunicaciones para gestionar su respaldo y periodicidad.

5.7.4. Registro y monitoreo

5.7.4.1. Registro de eventos

Todos los sistemas y aplicaciones críticos del CACES, bases de datos y dispositivos de red y servidores, deben contar con registros de eventos y bitácoras de seguridad protegidos debidamente.

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar e implementar un procedimiento para registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.

5.7.4.2. Protección de los registros de información

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar e implementar un procedimiento para proteger contra posibles alteraciones y accesos no autorizados la información de los registros. Además, se deben mantener respaldos periódicos de los registros de la información.

5.7.4.3. Registros de administración y operación

La Unidad de Tecnologías de la Información y Comunicaciones debe contar con un registro de las actividades de los operadores y administradores de los sistemas. Éstos deben incluir como mínimo lo siguiente:

- El tiempo en que ocurrió el evento.
- Detalles del evento o fallas en el mismo.
- Detalles de la cuenta de usuario y/o administrador implicado.

5.7.4.4. Sincronización de relojes

Todos los equipos de cómputo, sistemas, servidores, bases de datos y de comunicaciones que se encuentren en los dominios de red del CACES, deben estar sincronizados con una fuente común y exacta de tiempo (servidor NTP).

La Unidad de Tecnologías de la Información y Comunicaciones debe implementar y documentar procedimientos para que los cambios de horario no afecten la operación de la institución o a la exactitud de los registros de auditorías. Todos los equipos de cómputo y comunicaciones deben configurarse para que se sincronicen con el servidor NTP.

5.7.5. Control del software en producción

5.7.5.1. Instalación del software en sistemas en producción

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar, socializar e implementar una política para la restricción en la instalación de software. Asimismo, debe asegurarse que todo el software que se instale en los servidores y equipos de cómputo de cada servidor cuente con el licenciamiento vigente, suficiente para atender los requerimientos del CACES.

La Unidad de Tecnologías de la Información y Comunicaciones es responsable de administrar y resguardar las licencias del software institucional. Además, deben realizar por lo menos, los siguientes controles de seguridad:

- Todo el software que se instale en ambientes productivos debe ser previamente evaluado y probado en ambientes de pruebas.
- Ningún programador o analista de desarrollo y mantenimiento de aplicaciones podrá acceder a los ambientes de producción.
- Asignar un responsable de la implantación de cambios por sistema (no podrá ser personal que pertenezca al área de desarrollo o mantenimiento de aplicaciones).
- La instalación del software autorizado debe ser realizado por personal calificado, siguiendo los lineamientos de control de cambios y llevando un control estricto de las versiones.
- Todo el software que se instale en los equipos de cómputo del CACES debe estar inventariado en un catálogo de software institucional.
- Llevar un registro de auditoría de las actualizaciones realizadas.
- Retener las versiones previas del sistema, como medida de contingencia.

La Unidad de Tecnologías de la Información y Comunicaciones es la única instancia autorizada para instalar, actualizar y desinstalar el software de los equipos de cómputo.

5.7.6. Gestión de la vulnerabilidad técnica

5.7.6.1. Gestión de las vulnerabilidades técnicas

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar e implementar una política de monitoreo continuo sobre los sistemas en producción, detectar vulnerabilidades técnicas, adoptar las medidas necesarias para afrontar el riesgo asociado.

5.7.6.2. Restricciones en la instalación de software

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar, implementar y socializar la política que rija la instalación de software por parte de los usuarios.

Queda prohibido a los servidores públicos del CACES instalar y/o ejecutar software, sin previa autorización y cumplimiento de la política de instalación de software.

5.7.7. Consideraciones sobre la auditoría de sistemas de información

5.7.7.1. Controles de auditoría de sistemas de información

Los requisitos y las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deben ser cuidadosamente planificados y acordados para minimizar el riesgo de interrupciones en los procesos del CACES.

Se debe asegurar que la persona que realiza la auditoría sea independiente de las actividades auditadas, se dará acceso únicamente a lectura de la información. Se debe documentar todos los procedimientos, requisitos y responsabilidades de la auditoría, así como guardar los registros de su implementación.

5.8. Seguridad en las comunicaciones

5.8.1. Gestión de la seguridad de redes

5.8.1.1. Controles de red

La Unidad de Tecnologías de la Información y Comunicaciones debe establecer controles de seguridad para salvaguardar la confidencialidad y la integridad de los datos

que pasan por las redes públicas, redes locales e inalámbricas para proteger los sistemas y sus aplicaciones; así como para mantener la disponibilidad de las computadoras y los servicios de red del CACES conectados. Para esto se debe, por lo menos, efectuar los siguientes controles:

- Establecer las responsabilidades y los procedimientos para la administración de los equipos en la infraestructura de la red.
- Registro y monitoreo de eventos que permita registrar y detectar acciones que podrían afectar, o ser relevantes para la seguridad de la información.
- Autenticar el acceso a la red y a sus sistemas.
- La conexión de los sistemas a la red debe ser restringido de acuerdo con la criticidad y la gestión institucional.
- Establecer los procedimientos y responsabilidades para la gestión de equipos remotos como el caso de redireccionamiento de puertos y accesos por VPNs, incluyendo el área de operaciones y el área de usuarios finales.
- Contar con un esquema de red de los enlaces de datos, internet y redes locales, así como la documentación respectiva.

5.8.1.2. Seguridad de los servicios de red

La Unidad de Tecnologías de la Información y Comunicaciones debe identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deben incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la institución como si se subcontratan. Por tanto, la Unidad de Tecnologías de la Información y Comunicaciones debe implementar, por los menos, los siguientes controles:

- Incorporar tecnología aplicada para la seguridad de los servicios de red, como la autenticación, cifrada y controles de conexión de red.
- Implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red, como la implementación de firewalls, antivirus, entre otros.
- Establecer procedimientos para la utilización de los servicios de red para restringir el acceso a los mismos o a las aplicaciones, cuando sea necesario.
- Definir e implementar los parámetros técnicos para conexiones seguras, de acuerdo con la necesidad del CACES.

5.8.1.3. Separación en las redes

La Unidad de Tecnologías de la Información y Comunicaciones es la responsable de garantizar que las redes estén segregadas con base en los grupos de servicios de información, los usuarios, los sistemas de información y los activos de información críticos en función del riesgo que estos podrían presentar.

5.8.2. Transferencia de información

5.8.2.1. Políticas y procedimientos de transferencia de información

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar, implementar y socializar las políticas, procedimientos y controles formales que protejan el intercambio de información mediante el uso correcto de todo tipo de recursos de comunicación. En estos documentos se debe incluir, al menos, los siguientes controles de seguridad:

- Establecer procedimientos para proteger la información intercambiada contra la intercepción, copiado, modificación, errores de enrutamiento y destrucción.
- Definir procedimientos para detección y protección contra software malicioso que puede ser transmitido a través de comunicaciones electrónicas.
- Establecer controles por medio de técnicas criptográficas para proteger la confidencialidad, integridad y autenticidad de la información.
- Establecer procedimientos para el uso de las redes inalámbricas con base en los riesgos involucrados.

5.8.2.2. Acuerdos de transferencia de información

El presidente del CACES, el Oficial de Seguridad de la Información y/o el servidor delegado en la institución, podrán mantener contacto con cualquier otra institución pública o privada con la que se necesite establecer transferencias de comunicación. Estas comunicaciones deben reportarse al presidente del CACES.

Los acuerdos de transferencia de información que se establezcan deben considerar como mínimo los siguientes aspectos:

- Acuerdos sobre etiquetado de la información y la protección segura.
- Canales autorizados para la transferencia de la información.
- Definición de responsabilidades por incidentes de seguridad, divulgación o pérdida de información.

- Definir niveles mínimos de control de acceso.

5.8.2.3. Mensajería electrónica

La Unidad de Tecnologías de la Información y Comunicaciones debe generar y socializar políticas y procedimientos necesarios en la información de mensajería electrónica, de acuerdo con la norma legal vigente.

La Unidad de Tecnologías de la Información y Comunicaciones debe garantizar la disponibilidad y confiabilidad del correo electrónico institucional.

5.8.2.4. Acuerdos de confidencialidad o no revelación

La Procuraduría es la responsable de establecer y mantener actualizado el contenido de todos los acuerdos de confidencialidad y de no revelación de información, de acuerdo con las necesidades de la institución y las leyes vigentes. Los acuerdos de confidencialidad son aprobados por el presidente del CACES.

La Dirección de Administración de Talento Humano debe efectuar la divulgación y custodia del acuerdo de confidencialidad cuando se incorporen nuevos servidores públicos a la institución o para terceros que involucre el manejo de información del CACES.

5.9. Adquisición, desarrollo y mantenimiento de los sistemas de información

5.9.1. Requisitos de seguridad de los sistemas de información

5.9.1.1. Análisis de requisitos y especificaciones de seguridad de la información

Para el análisis de los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes, la Unidad de Tecnologías de la Información y Comunicaciones debe contemplar los controles de seguridad necesarios que deben estar documentados y evidenciar registros, para la protección de los activos involucrados, considerando la disponibilidad, la confidencialidad y la integridad de la información.

5.9.1.2. Asegurar los servicios de aplicaciones en redes públicas

La información involucrada en aplicaciones que pasan a través de redes públicas debe ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y

modificación no autorizadas. Para esto, la Unidad de Tecnologías de la Información y Comunicaciones debe establecer los mecanismos necesarios para la protección de la información, incluyendo como mínimo los siguientes aspectos:

- Credenciales de acceso a los sistemas institucionales.
- Establecer responsabilidades tanto para el que presta como para el que usa el servicio.
- Establecer acuerdos de confidencialidad e integridad.
- Implementar los controles necesarios que permitan proteger la información confidencial.
- Autenticación de transacciones.
- Trazabilidad de las operaciones.

5.9.1.3. Controles de transacciones en línea

La Unidad de Tecnologías de la Información y Comunicaciones debe implementar controles en las aplicaciones institucionales, para evitar transmisiones incompletas, errores de enrutamiento, alteración no autorizada, difusión, duplicación, o reproducción de mensajes no autorizados. Para esto debe considerar por lo menos los siguientes controles:

- Establecer procedimientos para el uso de certificados digitales (ejem.: firmas electrónicas) por las partes involucradas en la transacción.
- Definir procedimientos para que en todos los aspectos de la transacción se ejecuten controles de seguridad que garanticen la confidencialidad.
- Cifrar o encriptar el canal de comunicaciones entre las partes involucradas.
- Establecer protocolos seguros en la comunicación de las partes involucradas.
- Establecer procedimientos para que las transacciones se encuentren fuera del entorno de acceso público, que puede ser en una plataforma de almacenamiento existente en la intranet de la institución.
- Utilizar los servicios de una entidad certificadora confiable.

5.9.2. Seguridad en el desarrollo y en los procesos de soporte

5.9.2.1. Política de desarrollo seguro

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar, socializar e implementar en el área respectiva una política de desarrollo seguro de aplicaciones y

sistemas de la institución. Para esto deberá considerar, al menos, lo siguientes controles de seguridad:

- Implementar directrices de seguridad de acuerdo con el modelo de desarrollo del software, en el ciclo de vida del desarrollo, considerando: seguridad en la metodología de desarrollo de software y manual de desarrollo seguro para cada lenguaje de programación.
- Establecer los requisitos indispensables de seguridad en la fase de diseño.
- Adoptar las metodologías institucionales para el desarrollo de proyectos, incluyendo en los hitos puntos de verificación de seguridad.
- Seguridad en el control de versiones.

5.9.2.2. Procedimientos de control de cambios en sistemas

Todo cambio o modificación en ambiente productivo del software institucional, debe apegase al procedimiento de control de cambios de la Unidad de Tecnologías de la Información y Comunicaciones.

5.9.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo

Previo al inicio de la puesta en operación en ambiente productivo de un aplicativo se debe realizar el análisis de vulnerabilidades correspondiente, el cual debe realizarlo un tercero, distinto a quién lo desarrolló; el resultado del análisis debe presentarse al servidor público del nivel jerárquico superior o jefe de unidad para su consideración y liberación correspondiente.

Cuando se modifiquen o actualicen los sistemas operativos, estos deben contar con un periodo de pruebas documentado, a fin de que no existan efectos adversos en las operaciones o en la seguridad de la institución.

5.9.2.4. Restricciones a los cambios en los paquetes de software

Se debe evitar las modificaciones en el software suministrado o adquirido a terceros por el CACES, limitarse a cambios realmente necesarios; considerar un control estricto sobre los cambios.

En el caso excepcional que se vaya a efectuar algún cambio en los paquetes de software, se debe revisar los términos y condiciones de la licencia, a fin de determinar

si las modificaciones se encuentran autorizadas y si es el caso solicitar la autorización al jefe de la Unidad de Tecnologías de la Información y Comunicaciones para proceder.

5.9.2.5. Principios de ingeniería de sistemas seguros

La Unidad de Tecnologías de la Información y Comunicaciones debe establecer, documentar, mantener y guardar registros de la implementación de los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.

5.9.2.6. Ambiente de desarrollo seguro

La Unidad de Tecnologías de la Información y Comunicaciones debe establecer y proteger correctamente los ambientes de desarrollo seguro, para el desarrollo del sistema y los esfuerzos de integración, durante el ciclo de vida del desarrollo del sistema. Un ambiente de desarrollo seguro incluye las personas, los procesos y la tecnología relacionados con el desarrollo e integración del sistema. Para esto, se debe establecer entornos de desarrollo seguros para los proyectos específicos de desarrollo del sistema, considerando por lo menos lo siguiente:

- Evaluar los riesgos asociados con los proyectos de desarrollo de sistemas individuales.
- Considerar la criticidad de los datos a ser procesados, almacenados y transmitidos por el sistema.
- Aplicación de normativa legal vigente al respecto.
- Controles de seguridad que aseguren el desarrollo del sistema.
- Separación de los diferentes ambientes de desarrollo de ser necesario y procedente.
- Control de accesos al ambiente de desarrollo.
- Evaluar continuamente los cambios en el ambiente de desarrollo y el código almacenado en el mismo;
- Respaldos adecuadamente almacenados, almacenamiento seguro de las copias de seguridad.
- Control del movimiento de datos desde y hacia el ambiente.

5.9.2.7. Desarrollo externalizado

La Unidad de Tecnologías de la Información y Comunicaciones es la responsable de supervisar, monitorear y evaluar el cumplimiento de las condiciones de seguridad requeridas por el CACES a las actividades del desarrollo del sistema que se contrate.

5.9.2.8. Pruebas de seguridad del sistema

La Unidad de Tecnologías de la Información y Comunicaciones debe realizar pruebas exhaustivas de verificación de la funcionalidad y de aspectos de seguridad a los sistemas nuevos y a los actualizados en las etapas de desarrollo. Se deben realizar pruebas de aceptación independientes (tanto en los desarrollos internos como para los desarrollos externalizados) para asegurar que el sistema funciona como se esperaba y con los niveles de seguridad requeridos.

5.9.2.9. Pruebas de aceptación de sistemas

La Unidad de Tecnologías de la Información y Comunicaciones debe efectuar pruebas de aceptación y de seguridad para los sistemas de información nuevos o actualizados y nuevas versiones.

5.9.3. Datos de prueba

5.9.3.1. Protección de los datos de prueba

Los datos de prueba deben ser seleccionados cuidadosamente y se deberían proteger y controlar.

El encargado de este proceso en la Unidad de Tecnologías de la Información y Comunicaciones debe realizar una solicitud a su jefe para la autorización formal para realizar una copia de la base de datos de producción como base de datos de prueba. Al finalizar, el responsable debe eliminar inmediatamente, una vez completadas las pruebas, la información de producción utilizada.

5.10. Relaciones con proveedores

5.10.1 Seguridad de la información en la relación con los proveedores

5.10.1.1. Política de seguridad de la información en las relaciones con los proveedores

La Unidad de Tecnologías de la Información y Comunicaciones debe elaborar, socializar, implementar y guardar registros de la política de seguridad relacionada con el acceso del proveedor y terceras personas a los activos de información del CACES.

Debe documentarse formalmente los acuerdos con el proveedor para la mitigación de los riesgos asociados con el acceso. Para la creación de esta política se debe considerar, por lo menos, los siguientes aspectos:

- Establecer los tipos de acceso a la información que se permitirá a los diferentes tipos de proveedores
- Definir los requisitos mínimos de seguridad de la información por cada tipo de acceso a la información.
- Establecer los controles efectivos para garantizar la integridad de la información o del procesamiento de esta.
- Establecer el procedimiento necesario para el manejo de incidencias y contingencias asociadas al acceso de los proveedores, incluyendo responsabilidades, tanto de la institución, como de los proveedores.

5.10.1.2. Requisitos de seguridad en contratos con terceros

Cuando se efectúen contratos las áreas requirentes deben tomar en cuenta la política de seguridad relacionada con el acceso del proveedor y terceras personas a los activos de información del CACES.

En los contratos se deben incluir todos los requisitos de seguridad de la información, así como se debe establecer y acordar con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura IT.

Los proveedores o terceros deben firmar acuerdos de confidencialidad, para asegurar que la información y los activos de información de la institución a los que tengan acceso durante la relación laboral y después, no se divulgue sin autorización, ni sea utilizada o modificada en perjuicio de la institución.

5.10.1.3. Cadena de suministro de tecnologías de la información y de las comunicaciones

Los contratos con los proveedores o terceros deben incluir los requisitos para enfrentar los riesgos de seguridad de la información relacionados con las TICs, asociados con la cadena de suministros de los servicios y productos.

5.10.2 Gestión de la provisión de servicios del proveedor

5.10.2.1. Monitoreo y revisión de los servicios de proveedores

Los servidores públicos administradores de contratos deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor. Se deben mantener los registros del monitoreo y revisión.

En el caso de que se detecten faltas graves sobre la seguridad de la información incurridos por parte del proveedor se debe reportar inmediatamente al administrador del contrato y al Oficial de Seguridad de la Información del CACES.

5.10.2.2. Gestión de cambios en los servicios de proveedores

Se deben gestionar los cambios en la provisión de los servicios, que están ofreciendo los proveedores, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de la institución afectados, así como la reevaluación de los riesgos.

5.11. Gestión de incidentes de seguridad de la información

5.11.1. Gestión de los incidentes de seguridad de la información y mejoras

5.11.1.1. Responsabilidades y procedimientos

El Oficial de Seguridad de la Información debe establecer las responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y acorde con los incidentes de seguridad de la información que pueden ocurrir en la institución.

Estos procedimientos deben incluir, por lo menos, aspectos para: monitorear, detectar, analizar, comunicar, evaluar y tomar acciones correctivas sobre eventos e incidentes de seguridad de la información.

Las decisiones respecto a los incidentes de seguridad estarán a cargo del Pleno del CACES.

5.11.1.2. Reporte de los eventos de seguridad de la información

Es responsabilidad de todos los servidores públicos, personas sean naturales o jurídicas que tengan algún tipo de relación jurídica, laboral o contractual con el CACES y proveedores, notificar todos los eventos de seguridad por los canales establecidos en

el procedimiento de gestión de incidentes de seguridad de la información lo antes posible.

Se considerarán como situaciones para comunicar incidentes de seguridad de la información las siguientes:

- Control ineficaz de la seguridad de la información.
- Violación de las expectativas de integridad, confidencialidad y disponibilidad de la información.
- Errores humanos.
- Incumplimientos en la aplicación de políticas o directrices.
- Incumplimiento de las directrices de seguridad física.
- Cambios incontrolados del sistema.
- Fallas en el funcionamiento del software o hardware.
- Accesos no permitidos.

5.11.1.3. Reporte de debilidades de seguridad de la información

Todos los servidores públicos, personas sean naturales o jurídicas que tengan algún tipo de relación jurídica, laboral o contractual con el CACES y proveedores, deben obligatoriamente registrar y reportar, cualquier debilidad probable en la seguridad de la información, en los sistemas o servicios de información de la institución, tan pronto sea posible.

Cuando se detecte una vulnerabilidad o debilidad en un equipo, sistema o servicio se deberá ejecutar las siguientes acciones:

- Notificar al servidor público del nivel jerárquico superior o responsable de unidad y este al Oficial de Seguridad de la Información de la debilidad o vulnerabilidad detectada.
- Registrar la fecha, hora, apellidos y nombres del servidor que detectó la debilidad o vulnerabilidad, descripción de la debilidad, descripción de posibles incidentes de seguridad que pudieran ocurrir producto de esta debilidad. El responsable de llevar este reporte denominado "Reporte de vulnerabilidades o debilidades de la seguridad de la información" es el Oficial de Seguridad de la Información
- Nunca, por razón alguna, deberá intentar probar la debilidad o vulnerabilidad

detectada en la seguridad. El ensayo de las vulnerabilidades se podría interpretar como un posible uso inadecuado del sistema, equipo o servicio y también podría causar daño al sistema o servicio de información y eventualmente podría recaer en una responsabilidad legal.

- El Oficial de Seguridad de la Información deberá tomar las medidas pertinentes para prevenir o eliminar la vulnerabilidad o debilidad detectada.

5.11.1.4. Apreciación y decisión sobre los eventos de seguridad de la información

El Oficial de Seguridad de la Información con el responsable de la Unidad de Tecnologías de la Información y Comunicaciones deben evaluar los eventos de seguridad y determinar si corresponde a un incidente de seguridad de la información. Si es un incidente de seguridad se deberá identificar el impacto y el alcance.

5.11.1.5. Respuesta a incidentes de seguridad de la información

Cuando un incidente se produzca, el servidor responsable del equipo o sistema afectado debe realizar las siguientes acciones en el mismo orden:

- Levantamiento de evidencias del incidente inmediatamente.
- Registrar el incidente en una bitácora de incidentes (reporte de eventos) incluyendo fecha, hora, nombres y apellidos del servidor responsable, área afectada, equipo o sistema afectado y breve descripción del incidente.
- Notificar al del servidor público del nivel jerárquico superior o jefe de unidad y al Oficial de Seguridad de la información.
- Clasificar el incidente de acuerdo con el tipo de servicio afectado y al nivel de severidad.
- Asignar una prioridad de atención al incidente en el caso de que se produjeran varios en forma simultánea.
- Realizar un diagnóstico inicial, determinando mensajes de error producidos, identificando los eventos ejecutados antes de que el incidente ocurra, recreando el incidente para identificar sus posibles causas.
- El servidor debe escalar el incidente al servidor público del nivel jerárquico superior o jefe de unidad de inmediato. Al escalar el incidente se deberá registrar en la bitácora de escalamiento de incidentes.

- Investigar y diagnosticar en forma definitiva las causas por las cuales se produjo el incidente.
- Una vez que se haya resuelto el incidente por parte de la persona responsable se debe registrar el cierre en la bitácora incidentes como “Resuelto”.

5.11.1.6. Aprendizaje de los incidentes de seguridad de la información

Se debe utilizar el conocimiento obtenido para analizar y resolver incidentes de seguridad de la información, para reducir la probabilidad y/o impacto de incidentes en el futuro, aplicando los controles adecuados.

5.11.1.7. Recopilación de evidencias

En el procedimiento de gestión de incidentes de la seguridad de la información se deben incluir los criterios a considerar para identificar, recolectar, adquirir y conservar la información, que pueden servir de evidencia, conservando la misma de acuerdo con la norma legal vigente.

5.12. Aspectos de seguridad de la información para la gestión de la continuidad de las funciones del CACES

5.12.1. Continuidad de seguridad de la información

5.12.1.1. Planificación de la continuidad de seguridad de la información

El responsable de la Unidad de Tecnologías de la Información y Comunicaciones será el coordinador de la continuidad de los servicios informáticos, que se encargará de supervisar el proceso de elaboración e implantación del plan de continuidad de seguridad de la información, así como la Dirección de Administración de Talento Humano y la Coordinación General Administrativa Financiera, de la seguridad del plan personal.

Para la planificación de la continuidad de la seguridad de la información se deben identificar los activos involucrados en los procesos críticos de los servicios informáticos, así como de las actividades que se deben realizar.
El responsable de la Unidad de Tecnologías de la Información y Comunicaciones debe elaborar la política de continuidad de los servicios informáticos determinando los objetivos y el alcance del plan, así como las funciones y responsabilidades.

5.12.1.2. Implementación de la continuidad de seguridad de la información

El plan de continuidad de seguridad de la información debe detallar claramente la estructura de gestión adecuada y preparada para mitigar y responder a un evento disruptivo, usando el personal con la autoridad, experiencia y competencia necesarias. En este plan se deberá describir como la institución tratará la interrupción brusca y mantendrá la seguridad de la información.

Se debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

5.12.1.3. Verificar, revisar y evaluar la continuidad de seguridad de la información

Para verificar permanentemente los controles de continuidad de la seguridad de la información establecidos e implementados para garantizar su efectividad ante eventos adversos, se debe efectuar por lo menos las siguientes actividades:

- Evaluar la capacidad de respuesta.
- Ejecutar autoevaluaciones del plan de continuidad y establecer un plan de mejoras.
- Ejecutar y probar la funcionalidad de los procesos, procedimientos y controles para la continuidad de la seguridad de la información.

5.12.2. Redundancias

5.12.2.1. Disponibilidad de las instalaciones de procesamiento de la información

Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

5.13. Cumplimiento

5.13.1. Cumplimiento de los requisitos legales y contractuales

5.13.1.1. Identificación de la legislación aplicable y de los requisitos contractuales

Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deben definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.
Se debe considerar las normas y las leyes más generales relacionadas a la gestión de datos e información electrónica en el gobierno, como las siguientes:

- Constitución de la República del Ecuador.
- Ley de Comercio Electrónico. Firmas Electrónicas y Mensajes de Datos.
- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Ley del Sistema Nacional de Registro de Datos Públicos.
- Ley Orgánica y Normas de Control de la Contraloría General del Estado.
- Leyes y normas de control del sistema financiero.
- Ley del Sistema Nacional de Archivos.
- Código orgánico de la economía social de los conocimientos, creatividad e innovación.
- Otras normas cuya materia trate sobre la gestión de los activos de información en las instituciones de la Administración Pública.

5.13.1.2. Derechos de propiedad intelectual

La Procuraduría y la Unidad de Tecnologías de la Información y Comunicaciones deben elaborar, implementar y socializar una política para el cumplimiento de los derechos de propiedad intelectual, definiendo el uso legal de aplicativos y del software institucional.

5.13.1.3. Protección de los registros

La Unidad de Tecnologías de la Información y Comunicaciones debe implementar controles de seguridad apropiados para proteger los registros contra pérdida, destrucción y falsificación de la información.

La Unidad de Tecnologías de la Información y Comunicaciones debe asegurar que cada operación o actividad realizada por los usuarios de los aplicativos institucionales o sistemas, deje constancia electrónica.

5.13.1.4. Protección y privacidad de la información de carácter personal

La Procuraduría debe desarrollar, implementar y socializar la política de protección y privacidad de la información, según dispone la norma legal vigente.

El Oficial de Seguridad de la Información deberá controlar la aplicación de la política de protección de datos y privacidad de la información personal.

5.13.1.5. Reglamentos de controles criptográficos

La Unidad de Tecnologías de la Información y Comunicaciones debe establecer los controles de cifrado en cumplimiento con todos los acuerdos, leyes reglamentos de la legislación vigente. Asimismo, se debe restringir el uso de encriptación, y especificar y documentar los ámbitos en dónde se aplicarán tales procesos (ej., comunicaciones, firma de documentos, trasmisión de datos, entre otros).

5.13.2. Revisiones de seguridad de la información

5.13.2.1. Revisión independiente de seguridad de la información

La gestión de seguridad de la información debe ser revisada al menos 1 vez al año, o cuando se produzcan cambios significativos en la institución por parte del Comité de Seguridad de la Información.

5.13.2.2. Cumplimiento de las políticas y normas de seguridad

Los servidores públicos del CACES tienen la obligación de adoptar cualquier regulación en materia de seguridad de la información, que sea aplicable a la institución, o bien, cualquier normatividad que sea aprobada.

Los servidores públicos del nivel jerárquico superior y responsables de unidad deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.

5.13.2.3. Comprobación del cumplimiento técnico

Para comprobar regularmente que los sistemas de información cumplen con las políticas y normas de seguridad de la información de la institución, deben ser calendarizadas y planeadas para prevenir interrupciones en la operación. Los requerimientos y el alcance de las revisiones serán acordados con el Comité de Seguridad de la Información.

6. Documentos de referencia

Los documentos a los cuales se hace referencia en la Política son:

- Acuerdo Ministerial 025-2019
- Esquema Gubernamental de Seguridad de la Información (EGSI v2.0)
- Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001.
- Ley Orgánica de Transparencia y Acceso a la información Pública Ley 24 del Registro Oficial Suplemento 337 de 18-may.-2004.

7. Terminología

Los términos/palabras técnicas que se usan en este documento son:

- Activo de información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la institución.
- Amenaza: causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.
- Análisis de riesgos: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- Aplicación: solución de TI, incluyendo programas de aplicación, datos de aplicaciones y procedimientos diseñados para ayudar a los usuarios de las organizaciones a realizar tareas específicas o manejar tipos específicos de problemas de TI, automatizando un proceso o función del negocio.
- Ataque: intento de destruir, exponer, alterar, deshabilitar, robar o lograr acceso no autorizado o hacer uso no autorizado de un activo.
- Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta.
- Autenticidad: Propiedad de que una entidad es lo que afirma ser.
- Confidencialidad: la información solo tiene que ser accesible o divulgada a aquellos que están autorizados.
- Comité de Seguridad de la información (CSI): se encarga de gestionar la

implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información.

- Control: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- Disponibilidad: la información debe estar siempre accesible para aquellos que estén autorizados.
- Evaluación de riesgos: proceso global de identificación, análisis y estimación de riesgos.
- Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
- Identificación de riesgos: proceso de encontrar, reconocer y describir riesgos.
- Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- Información: es uno de los activos más importantes de las Instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.
- Integridad: la información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.
- Software malicioso: software diseñado con malas intenciones que contiene características o capacidades que potencialmente pueden causar daño directa o indirectamente al usuario y/o al sistema informático del usuario.
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- Responsable del activo de información: es el propietario del activo y su custodio.
- Seguridad de la información: conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información.

- Sistema de información: aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento.
- Tratamiento de riesgos: proceso de modificar el riesgo, mediante la implementación de controles.
- Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas.

8. Acrónimos

- EGSI: Esquema Gubernamental de Seguridad de la Información para las instituciones de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva (APCID) para preservar la integridad, disponibilidad y confidencialidad de la información.
- CSI: Comité de Seguridad de la Información.
- OSI: Oficial de Seguridad de la Información.

RESOLUCIÓN No. SB-DTL-2021-1736

LUIS ANTONIO LUCERO ROMERO
DIRECTOR DE TRÁMITES LEGALES

CONSIDERANDO:

QUE mediante comunicación ingresada electrónicamente en el Sistema de Calificaciones con hoja de ruta No. SB-SG-2021-44405-E, el Ingeniero Civil Washington Orlando López Escobar, con cédula No. 1804642856, solicitó la calificación como perito valuador en el área de bienes inmuebles, entendiéndose que la documentación remitida a la Superintendencia de Bancos es de responsabilidad exclusiva de la parte interesada, que es auténtica y no carece de alteración o invalidez alguna;

QUE el numeral 24 del artículo 62 del Código Orgánico Monetario y Financiero, establece dentro de las funciones otorgadas a la Superintendencia de Bancos, la calificación de los peritos valuadores;

QUE el artículo 4 del capítulo IV "Normas para la calificación y registro de peritos valuadores", del título XVII "De las calificaciones otorgadas por la Superintendencia de Bancos", del libro I "Normas de control para las entidades de los sectores financieros público y privado", de la Codificación de las Normas de la Superintendencia de Bancos, establece los requisitos para la calificación de los peritos valuadores;

QUE el inciso quinto del artículo 6 del citado capítulo IV, establece que la resolución de la calificación tendrá una vigencia de diez (10) años contados desde la fecha de emisión de la resolución;

QUE mediante memorando No. SB-DTL-2021-1883-M de 23 de septiembre del 2021, se ha determinado el cumplimiento de lo dispuesto en la norma citada; y,

EN ejercicio de las atribuciones delegadas por el señor Superintendente de Bancos mediante resolución No. SB-2019-280 de 12 de marzo del 2019; y, resolución No. ADM-2021-14787 de 17 de febrero del 2021,

RESUELVE:

ARTÍCULO 1.- CALIFICAR al Ingeniero Civil Washington Orlando López Escobar, con cédula No. 1804642856, como perito valuador en el área de bienes inmuebles en las entidades sujetas al control de la Superintendencia de Bancos.

ARTÍCULO 2.- VIGENCIA, la presente resolución tendrá vigencia de diez (10) años, contados desde la fecha de emisión, manteniendo su número de registro No. PVQ-2021-02230.

ARTÍCULO 3.- COMUNICAR a la Superintendencia de Compañías, Valores y Seguros con la presente resolución.

COMUNÍQUESE Y PUBLÍQUESE EN EL REGISTRO OFICIAL.- Dada en la Superintendencia de Bancos, en Quito, Distrito Metropolitano, el veintitrés de septiembre del dos mil veintiuno.

Mgs. Luis Antonio Lucero Romero
DIRECTOR DE TRÁMITES LEGALES

LO CERTIFICO.- Quito, Distrito Metropolitano, el veintitrés de septiembre del dos mil veintiuno.

Dra. Silvia Jeaneth Cástro Medina
SECRETARIA GENERAL

SUPERINTENDENCIA DE BANCOS
CERTIFICO QUE ES FIEL COPIA DEL ORIGINAL

SILVIA JEANETH CASTRO MEDINA

Firmado digitalmente por SILVIA JEANETH CASTRO MEDINA
Fecha: 2021.09.24 09:45:36 -05'00'

Dra. Silvia Jeaneth Castro
SECRETARIA GENERAL

Ing. Hugo Del Pozo Barrezueta
DIRECTOR

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Telf.: 3941-800
Exts.: 3131 - 3134

www.registroficial.gob.ec

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

"Al servicio del país desde el 1º de julio de 1895"