RESOLUCIÓN N°. DE

"**Por la cual se establecen los Objetivos, Política General y Políticas Específicas del Sistema de Gestión de Seguridad de la Información en la Unidad para la Atención y Reparación Integral a las Víctimas- UARIV- y se deroga la Resolución No 740 del 11 de noviembre de 2014"**

EL DIRECTOR GENERAL

DE LA UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS

En uso de sus facultades legales y reglamentarias otorgadas por la Ley 1448 de 2011, el Decreto 4802 de 2011, y

CONSIDERANDO:

Que el inciso primero del artículo 15 de la Constitución Política establece que: *"Todas las personas tienen derecho a su intimidad personal, familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"*

Que la Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones (…)"

Que el artículo 1 de la Ley Estatutaria No 1712 de 2014 relacionada con la Transparencia y el Derecho de Acceso a la Información Pública Nacional, tiene por objeto: "*regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información."*

Que el literal a) del artículo 6 ibídem define la información como: " un *conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen";* y así mismo en los literales que se relacionan a continuación realiza la siguiente clasificación:

> *"b)* ***Información pública.*** *Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal;*
>
> *c)* ***Información pública clasificada.*** *Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley;*
>
> *d)* ***Información pública reservada.*** *Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley*
>
> *(…)"*

Que, de acuerdo con lo anterior, dicha normatividad consagra los instrumentos de gestión para información pública a través de: i. Registro de Activos de Información; ii. Índice de Información Clasificada y Reservada y iii. Esquema de Publicación de Información.

Que la Ley Estatutaria No 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" reviste un tratamiento especial y conforme al artículo 17 de dicha normatividad se señalan los deberes del responsable respecto al tratamiento de datos dentro de los cuales se destacan los siguientes literales:

> "a) *Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data*"
>
> (…)
>
> (…)
>
> "*d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".*

Que la Ley 1448 de 2011 "Por la cual se dictan medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno y se dictan otras disposiciones" en su artículo 166, crea la Unidad para la Atención y Reparación Integral a las Víctimas, como una Unidad Administrativa especial con personería jurídica y autonomía administrativa y patrimonial y a través del artículo 29 dispone que:

> "(…)
>
> *Las autoridades garantizarán la confidencialidad de la información suministrada por las víctimas y de manera excepcional podrá ser conocida por las distintas entidades que conforman el Sistema Nacional de Atención y Reparación de las Víctimas para lo cual suscribirán un acuerdo de confidencialidad respecto del uso y manejo de la información".*

Que los datos e información que se genere obtengan, use o se almacene, custodie, distribuya, envie, intercambie y/ o modifique en la Unidad para la Atención y Reparación Integral a las Víctimas, en cada uno de sus procesos misionales, de apoyo y estratégicos son sensibles y deben manejarse en condiciones que garantice su confiabilidad, oportunidad y seguridad.

Que el artículo 2.2.9.1.1.1 de**l** Decreto 1078 de 2015 subrogado por el artículo 1 del Decreto 1008 de 2018 señala: *"los lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital".*

Que el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 subrogado por el artículo 1 del Decreto 1008 de 2018 dispone que: "la Política de Gobierno Digital será definida por el Ministerio de Tecnologías de la Información y las Comunicaciones y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC, conforme se describe a continuación:

> (…)
>
> (…)
>
> 1. Componentes de la Política de Gobierno Digital: Son las líneas de acción que orientan el desarrollo y la implementación de la Política de Gobierno Digital, a fin de lograr sus propósitos. Los componentes son:
> 1.1. TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones.

1.2. TIC para la Sociedad: Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común.
2. Habilitadores Transversales de la Política de Gobierno Digital: Son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.
3. Lineamientos y estándares de la Política de Gobierno Digital: Son los requerimientos mínimos que todos los sujetos obligados deberán cumplir para el desarrollo de los componentes y habilitadores que permitirán lograr los propósitos de la Política de Gobierno Digital.
4. Propósitos de la Política de Gobierno Digital: Son los fines de la Política de Gobierno Digital, que se obtendrán a partir del desarrollo de los componentes y los habilitadores transversales, estos son:
4.1. Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.
4.2. Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.
4.3. Tomar decisiones basadas en datos a partir del aumento, el uso y aprovechamiento de la información.
4.4. Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto.
4.5. Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC"

Que el artículo 2.2.9.1.1.3 del Decreto 1008 de 2018 **"**Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" establece los principios de la Política de Gobierno Digital siendo uno de ellos, la Seguridad de la Información que busca:

"*crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano".*

Que el documento CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital, la cual contiene entre otros, principios fundamentales relacionados con: "*PF1. Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos en Colombia, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de la intimidad y los datos personales y la privacidad, así como los principios fundamentales consagrados en la Constitución Política de Colombia. (…)* y "*PF4. Adoptar un enfoque basado en la gestión de riesgos, que permita a los individuos el libre, seguro y confiable desarrollo de sus actividades en el entorno digital. (…)".*

Que mediante el CONPES 3995 de 2020 establece la Política Nacional de Confianza y Seguridad Digital, la cual tiene como objetivo: "*Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías*"

Que el artículo 2.2.9.1.2.1 del Decreto 1008 de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" al señalar la estructura respecto a la Política de Gobierno Digital establece la seguridad de la información como elemento fundamental y habilitador transversal de la referida política.

Que la Directiva Presidencial 03 de 2021 señala entre otros aspectos, los lineamientos de Seguridad Digital, siendo relevantes:

> "3.1. "*Dar cumplimiento a las directrices en materia de seguridad digital y de la información que expida el MinTIC y las que se expidan en el marco de la política nacional de confianza y seguridad digital del Gobierno Nacional (…)*
>
> *3.2. (…) fortalecer las medidas en materia de seguridad digital considerando las dinámicas que ha incorporado el uso de medios digitales: (…)"*

Que el artículo 1 de la Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" expedida por el MINTIC tiene por objeto: *"establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.*

Que la Norma ISO 27001:2013 suministra requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de Gestión de Seguridad de la Información.

Que mediante la Resolución No 569 de 2018 la Unidad para la Atención y Reparación Integral a las Víctimas adoptó y actualizó el Sistema Integrado de Gestión involucrando varios sistemas dentro de los cuales se encuentra el Sistema de Seguridad de la Información bajo la Norma Técnica ISO 27001:2013.

Que según el artículo 6 de la resolución referida, el líder del Sistema de Gestión de Seguridad de la Información se encuentra a cargo de la Oficina de Tecnologías de la Información.

Que la Oficina de Tecnologías de la Información de la Entidad tiene a su cargo el desarrollo de la Arquitectura Empresarial la cual consiste en la alineación de los datos, procesos, sistemas de información e infraestructura; y reviste importancia toda vez, que señala entre otros, los principios para el manejo y seguridad de la información. Dichos principios fueron aprobados por la Mesa de Gobierno Digital según acta del 30 de octubre de 2020.

Que el Artículo 2.2.9.1.3.3 del Decreto 1008 de 2018 señala que el Comité Institucional de Gestión de Desempeño, es el responsable de orientar la implementación de la política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.

Que el artículo 2.2.22.3.8 del Decreto 1083 de 2015 establece las funciones del Comité Institucional de Gestion y Desempeño, al cual se le adicionan las correspondientes a los comités que integra y/o sustituye; constituyéndose en una instancia que orienta no solamente la implementación del Modelo Integrado de Planeación y Gestión, sino también cada una de las políticas de Gestión y Desempeño necesarias para la mejora de los resultados y calidad en la prestación de servicios a los usuarios de la entidad.

Que según lo señalado por el Departamento Administrativo de la Función Pública en el Manual Operativo del Modelo Integrado de Planeación y Gestión -MIPG- "es viable la conformación de los equipos técnicos de apoyo al Comité Institucional de Gestión y Desempeño para la formulación de estrategias de operación y articulación al interior de la entidad".

Que la Unidad para la Atención y Reparación Integral a las Víctimas a través del Comité Directivo del 18 de junio de 2018, dio viabilidad para la creación de la Mesa de Gobierno Digital cuyo propósito será el cumplimiento de los logros establecidos en el marco de la Política y Estrategia de Gobierno Digital.

Que la Mesa de Gobierno Digital es la encargada de articular y consensuar las acciones y soluciones que se relacionan con la política de Gobierno Digital, para la aprobación posterior por parte del Comité Institucional conforme a las funciones asignadas a la mesa de Gobierno Digital según la Circular Interna No 0036 de 2020.

Que conforme a lo expuesto en párrafos precedentes es necesario para esta Entidad establecer los objetivos, política General y las Políticas Específicas orientadas al aseguramiento de la información respecto al manejo y uso de esta última por motivos de protección en términos de confidencialidad, integridad y disponibilidad frente a eventuales riesgos que se pueden configurar en la operación de la Unidad.

Que, en mérito de lo expuesto,

RESUELVE

CAPITULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto. La presente Resolución tiene como objeto establecer la política general del Sistema de Gestión de Seguridad de la Información y sus políticas específicas, así como definir los lineamientos frente al uso y manejo de la información de la Unidad para la Atención y Reparación Integral a las Víctimas.

Artículo 2 . Política General del Sistema de Gestión de Seguridad de la Información: La Unidad para la Atención y Reparación Integral a las Víctimas gestiona, controla y salvaguarda la confidencialidad, integridad y disponibilidad de la información de los procesos y de la población víctima, mediante la gestión de riesgos de seguridad de la información y la implementación de controles físicos y digitales para prevenir incidentes, promover la continuidad de las operaciones y desarrollar la cultura de seguridad de la Información.

De igual manera, pretende cumplir con la normatividad vigente y otras disposiciones en el marco de la mejora continua del mencionado sistema.

Artículo 3. **Objetivos del Sistema de Gestión de Seguridad de la Información**. La Unidad para las víctimas tiene como objetivos del sistema los siguientes:

I. Proteger la información y sistemas de información, según estándares que salvaguarden la confidencialidad, integridad y disponibilidad, de los activos de la Entidad.
II. Implementar los controles de seguridad de la información para mitigar, reducir o eliminar la divulgación, pérdida o modificación no controlada de los activos de la Entidad.
III. Realizar seguimiento a los eventos e incidentes de seguridad para obtener lecciones aprendidas y mejorar periódicamente el sistema de gestión de Seguridad de la Información.
IV. Promover, mantener y establecer la cultura de seguridad de la información en la Unidad para las Víctimas y partes interesadas.
V. Incrementar la disponibilidad de servicios de TI y de operación, a través del plan de continuidad de negocio.
VI. Suministrar información confiable, íntegra, oportuna, accesible y de valor a la población Víctima.

CAPITULO II

POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Artículo 4. **Política de organización interna**. Esta política consiste en la articulación o coordinación de los procesos estratégicos, misionales y de apoyo de la -UARIV- para asegurar la información en un escenario de corresponsabilidad.

Por consiguiente, con relación al dominio **A.6 *"Organización de la seguridad de la información"* del Anexo A de la ISO/IEC 27001:2013,** la Oficina de Tecnologías de la Información – (en adelante **OTI**) - tienen la responsabilidad de:

1. Establecer los roles y responsabilidades para asegurar la información, en articulación con los diferentes procesos que la gestionan.
2. Generar y mantener actualizado un listado de contactos, autoridades y grupos de interés de seguridad de la información para gestionar eficientemente las diferentes actividades de Seguridad de la información.
3. Apoyar en identificar, evaluar y tomar acciones para mitigar los riesgos en los proyectos y operaciones que impacten la información de los procesos y de la población víctima.

Artículo 5. Política de dispositivos móviles y trabajo en casa. Esta política consiste en garantizar que la información de la Unidad para las Víctimas se maneje en condiciones seguras desde dispositivos móviles o fuera de las instalaciones de la Entidad. Por consiguiente, con relación al dominio A.6 *"Organización de la seguridad de la información"* y controles A.6.2.1 "Política de dispositivos móviles" y A.6.2.2 "Teletrabajo" del Anexo A de la ISO/IEC 27001:2013, se establece que:

Es responsabilidad de la OTI en articulación con la Oficina Asesora de Comunicaciones divulgar las recomendaciones sobre el uso de servicios informáticos en las instalaciones y bajo la modalidad de trabajo en casa.

De igual manera, es responsabilidad de los usuarios que manejan información de la Unidad a través de dispositivos móviles utilizados en la modalidad de trabajo en casa, seguir los siguientes lineamientos:

1. Participar en las jornadas de sensibilización en seguridad y privacidad de la información.
2. Actualizar periódicamente las contraseñas.
3. Conocer y aplicar los procedimientos de seguridad de la información.
4. Usar software licenciado y autorizado por la Unidad para las Víctimas en los equipos de cómputo proporcionados por la Entidad.
5. Usar las herramientas dispuestas y/o aprobadas por la OTI para el manejo de la información sensible de la Entidad.
6. Firmar el acuerdo de confidencialidad de la información para el acceso y uso de la información sensible de la Entidad.
7. Dar buen uso del servicio de correo electrónico, mensajería, video conferencia, repositorios de almacenamiento e intercambio de información y acceso a la red (VPN) proporcionado por la Entidad.

Artículo 6. Política de seguridad de los recursos humanos. Esta política consiste en garantizar que los funcionarios, contratistas y/o colaboradores comprendan sus responsabilidades frente al aseguramiento de la información. Por consiguiente, con relación al dominio A.7 *"Seguridad de los recursos humanos"* del Anexo de la ISO/IEC 27001:2013 ", se establece que:

La Entidad debe contratar el personal idóneo con el propósito de asegurar la comprensión sobre su responsabilidad respecto a las políticas y lineamentos en materia de seguridad de la información. Esto para reducir los riesgos de hurto, fraude, filtraciones o uso inadecuado de la información en los equipos empleados en su tratamiento.

Lo anterior, según los siguientes lineamientos:

1. El grupo de Gestión de Talento Humano debe verificar la documentación sobre los antecedentes, las referencias laborales y los soportes de experiencia del personal en procesos de selección para vacantes de planta.

2. El área de la -UARIV- responsable del proceso de contratación del personal bajo la modalidad de prestación de servicios debe verificar los antecedentes, las referencias laborales y los soportes de experiencia relacionada del contratista.
3. Todos los funcionarios, contratistas y colaboradores deben reportar a través de los canales definidos por la Entidad, cualquier caso de fuga, modificación no autorizada o pérdida de información sensible que se encuentre almacenada en el equipo de cómputo.
4. El funcionario, contratista o colaborador es responsable de la información que produzca u obtenga, así como de los recursos tecnológicos y de software asignados por la Entidad.
5. Los funcionarios, contratistas y colaboradores con relación contractual a través de terceros deben conocer y aplicar las políticas, lineamientos, procedimientos y recomendaciones de seguridad de la información de la Entidad.
6. Se prohíbe a los usuarios realizar copias no autorizadas de información o software (código fuente o archivos compilados) de la Entidad.
7. No está permitido para ningún usuario realizar actividades tales como: borrar, alterar o eliminar información de la Entidad de manera no controlada o sin autorización, de tal forma que se afecte la operación de la Unidad.
8. Los funcionarios, contratistas y colaboradores de la Unidad deben usar los activos de la Entidad, únicamente para el cumplimiento de sus funciones en el marco de la misión institucional.
9. Los funcionarios, contratistas y colaboradores de la Unidad para las Víctimas no deben divulgar la información clasificada o reservada, en lugares públicos o privados mediante conversaciones o situaciones que puedan comprometer la seguridad o el buen nombre de la Entidad.
10. Los funcionarios, contratistas y colaboradores de la -UARIV- deben asistir a los escenarios de sensibilización en seguridad de la información cuando sean requeridos.
11. Es responsabilidad de los usuarios realizar copia de respaldo de la información sensible para la Entidad almacenada en equipos de cómputo o dispositivos móviles teniendo en cuenta los mecanismos dispuestos por la OTI (OneDrive y SharePoint).
12. Los funcionarios, contratistas y colaboradores de la -UARIV- no deben utilizar sus cuentas de correo personal para manejar información de la Entidad.
13. Los funcionarios, contratistas y colaboradores de la -UARIV- no deben manipular los dispositivos de almacenamiento interno o cualquier otro componente interno de los equipos de cómputo y dispositivos que sean asignados por la Entidad. Solamente el personal de soporte técnico calificado y autorizado por la -OTI- puede realizar estos procedimientos.
14. Todo funcionario, contratista y colaborador debe registrar el ingreso y salida de elementos tecnológicos en la bitácora de ingreso (solicitados por el personal de seguridad) en las instalaciones de la Entidad.
15. Para el proceso de desvinculación o cambio de rol:

    - La gestión de inactivación de los privilegios de acceso sobre los sistemas de información y/o herramientas de la UARIV en el caso de los funcionarios estará a cargo del jefe directo o para contratistas será el supervisor del contrato, o el enlace designado (según procedimiento de acuerdo de Confidencialidad).
    - Todo funcionario, contratista y colaborador que se retire de la Entidad o cambie de dependencia o rol, debe elaborar un acta entrega dirigida al jefe de la dependencia o supervisor del contrato de cualquier activo de información mantenido, usado o producido durante su vinculación con la entidad.
    - Los funcionarios, contratistas y colaboradores deben salvaguardar y proteger los activos asignados para el desempeño de sus labores u obligaciones. En caso que que dichos activos hayan sufrido algún tipo de daño debe establecerse la causa que lo originó para

determinar los correctivos o eventuales sanciones a que haya lugar, según sea el caso. Estas últimas en el marco del debido proceso.

Artículo 7. **Política de gestión de activos**. Esta política consiste en identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la misma.

Por consiguiente, con relación al dominio A.8 *"Gestión de activos"* del Anexo A de la ISO/IEC 27001:2013, la Unidad para las Víctimas establece que:

El propietario de la información o los responsables de procesos de la Entidad deben mantener el inventario de activos actualizado anualmente identificando el responsable en su generación, administración y/o custodia a nivel de proceso. Así mismo, deben clasificar los activos con relación a los niveles de acuerdo al tipo de información (pública, reservada o clasificada).

Lo anterior, según los siguientes lineamientos:

1. La información debe ser clasificada en función de la criticidad o susceptibilidad respecto a la divulgación, pérdida o modificación no autorizada.
2. Se debe etiquetar la información física o digital que genere la Entidad como información pública, reservada o clasificada. Esto aplica a los correos electrónicos e información documentada administrada por el proceso de gestión documental. Los comunicados públicos de la Entidad no requieren ser etiquetados.
3. Todos los funcionarios, contratistas y colaboradores deben proteger la información almacenada en dispositivos con relación a su acceso, uso, transporte, almacenamiento y eliminación, acorde con su nivel de clasificación.
4. Los dispositivos removibles asignados a los funcionarios, contratistas y colaboradores de la Entidad deben ser devueltos en los términos y condiciones definidas al momento de la asignación.

Artículo 8. Política de control de acceso. Esta política consiste en la identificación e implementación de controles que limiten el acceso a la información y a las instalaciones donde se procesa.

Por consiguiente, con relación al dominio A.9 *"Control de acceso"* del Anexo A de la ISO/IEC 27001:2013, se establece que:

El acceso a los activos de información de la- UARIV -se permite únicamente al personal autorizado ya sea con vinculación laboral o contractual vigente, en caso de usuarios internos o con acuerdo de intercambio de información entre las entidades para usuarios externos y/o proveedores. De acuerdo con los siguientes lineamientos:

1. El personal que tiene privilegios de acceso a los sistemas de información debe contar con vinculación laboral o contractual vigente con la Unidad para las Víctimas o con terceros que tengan contrato actual con la entidad y autorización de acceso al activo.
2. En el caso de las entidades públicas o privadas se debe establecer un acuerdo de intercambio de información para el acceso a la información de la entidad.
3. El acceso a los sistemas de información de los usuarios que son contratados a través de terceros (contratistas de la entidad o entidades externas) requiere diligenciar la correspondiente autorización o acuerdo de confidencialidad.
4. Los usuarios de entidades externas deben contar con la autorización de su colaborador designado, definido en el marco del acuerdo de intercambio de información y la autorización del proceso propietario del activo.
5. Se deben ejecutar los procedimientos por parte de las áreas correspondientes para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información.

6. Las credenciales de acceso a los sistemas de información de la Entidad deben ser individuales y es responsabilidad de los usuarios no compartirlas.
7. El manejo indebido de las credenciales de uso es responsabilidad del usuario asignado y será a quien se le solicite las explicaciones pertinentes por el uso inadecuado.
8. Las contraseñas de los usuarios deben cumplir con los siguientes parámetros:
    - Deben tener una longitud mínima de 8 caracteres alfanuméricos.
    - Deben contener al menos un número, una letra minúscula, una mayúscula y un carácter especial #$%()¡
    - Las contraseñas son de uso personal y por ningún motivo se debe divulgar a otros usuarios.
    - Se deben cambiar una vez se notifique la creación o asignación de credenciales de acceso genéricas.
    - Posteriormente deben ser cambiadas mínimo cada 2 meses.
9. Para la creación de los usuarios a través de sistemas de información o directorio activo, se entregará una contraseña temporal al usuario por medio de correo electrónico o llamada telefónica. Es responsabilidad del usuario cambiarla desde su primer uso.
10. Se debe reportar a través de soporte.oti@unidadvictimas.gov.co cualquier caso que evidencie el uso compartido de credenciales de acceso a herramientas tecnológicas.
11. Los usuarios no deben usar las credenciales de acceso de otros usuarios, ni intentar apoderarse de sus claves, tampoco probar una cantidad de combinaciones posibles con el fin de identificar contraseñas de usuarios legítimos para acceder a un Sistema de Información o equipo de cómputo de la Entidad.
12. Se deben generar registros de auditoría respecto al ingreso en los Sistemas de Información críticos de la Unidad para las Víctimas -UARIV-.
13. Se debe controlar el acceso a los registros de auditoría de sistemas de información para que solamente el personal autorizado, pueda acceder a ellos en el marco administración de la plataforma tecnológica.
14. Los sistemas de información de la UARIV deben contar con mecanismos de identificación individual de los usuarios y procedimientos para el control de acceso a los mismos. En caso de credenciales de acceso generadas en sistemas de información, para el acceso por parte de otros sistemas (interoperabilidad o intercambio de información), estas deben ser nombradas de manera genérica, una por cada sistema de información.
15. En caso de pérdida, robo, daño, alteración, divulgación no autorizada y/o fuga de información física o digital como consecuencia del descuido o actuación riesgosa por parte de un funcionario, contratista o colaborador de la Entidad, este último asumirá las sanciones a que haya lugar (disciplinarias o derivadas del contrato).
16. Los usuarios no deben acceder a la información de la Entidad sin firma previa del acuerdo o compromiso de confidencialidad.
17. El jefe inmediato o el supervisor del contrato según sea el caso, deberá informar al proceso de Gestión Administrativa y/o Gestión del talento humano, así como a los administradores de sistemas de información involucrados, las novedades relacionadas con el retiro o traslado del funcionario, contratista o colaborador de la Entidad.

Artículo 9. Política de criptografía. Esta política consiste en la implementación de técnicas de cifrado, cuando sea necesario, para proteger la información de la Entidad.

Por consiguiente, con relación al dominio A.10 *"Criptografía"* del Anexo A de la ISO/IEC 27001:2013 se establece:

El responsable del almacenamiento y/o transporte de información crítica confidencial debe usar controles criptográficos (discos cifrados), en caso de que sea necesario, definidos en el marco del sistema de gestión de seguridad de la información, de acuerdo con los siguientes lineamientos:

1. La Oficina de Tecnologías de la Información se encarga de administrar la plataforma para generar certificados digitales en la implementación del protocolo SSL en sitios o herramientas Web de la Entidad.
2. La Oficina de Tecnologías de la Información se encarga de administrar los discos duros cifrados, en el marco del procedimiento "Gestión de préstamo de discos duros cifrados".
3.

Artículo 10. Política de seguridad física y del entorno. Esta política consiste en la definición e implementación de controles relacionados con la seguridad física en las instalaciones de la Entidad. Por consiguiente, con relación al dominio A.11 *"Seguridad física y del entorno"* del Anexo A de la ISO/IEC 27001:2013, se establece que:

El proceso de gestión administrativa debe implementar los controles para el acceso físico a las instalaciones de la Entidad. Lo anterior con el fin de prevenir la pérdida de activos de la Entidad, el daño o interceptación de la información almacenada en medios físicos, bien sea en archivo o bodega de la Entidad. Para ello téngase en cuenta los siguientes lineamientos:

1. No se permite comer, consumir líquidos o fumar cerca de las instalaciones para procesamiento de información o centros de cableado.
2. El proceso de Gestión Administrativa debe hacer seguimiento de las condiciones requeridas de suministro eléctrico y condiciones ambientales tales como: temperatura y humedad para determinar los escenarios que puedan afectar negativamente la operación de las instalaciones de procesamiento de información o centros de cableado.
3. El cableado de energía eléctrica y datos debe estar debidamente protegido para evitar la interceptación, interferencia o daño, por medio de canaletas o bandejas definidas para tal fin. Es responsabilidad de todos los funcionarios, contratistas y colaboradores informar el incumplimiento de este numeral.
4. No se permite tomar fotografías o videos dentro de las instalaciones de procesamiento de información o centros de cableado sin la autorización de la OTI.
5. La configuración de máquinas de copiado o multifuncionales está permitida únicamente a personal técnico autorizado por la OTI.
6. El Grupo de Gestión Administrativa autorizará la salida de equipos y expedientes físicos de la Entidad.
7. La OTI debe realizar el borrado seguro de la información almacenada en discos duros (portables o de equipos de cómputo) que se entreguen al proveedor de servicios o que se reasignen a otro usuario para su uso.
8. Los usuarios deben retirar de forma inmediata todos los documentos confidenciales que envíen a las impresoras. No se debe reutilizar papel que contenga información confidencial o privada.
9. Es responsabilidad de los funcionarios, contratistas y colaboradores:
    - Mantener los equipos de acuerdo con las especificaciones de los fabricantes.
    - Registrar las fallas y mantenimientos correctivos, como evidencia de la gestión.
    - Usar la contraseña de control de impresión
    - Contar con un inventario detallado del Hardware y del Software presente en los equipos de cómputo.

- Verificar que el mantenimiento preventivo o correctivo es realizado por el personal calificado y autorizado por la OTI.

- El retiro inmediato de documentos impresos de las impresoras

10. La OTI debe programar actividades de mantenimiento periódico en los equipos que se encuentren en la modalidad de arrendamiento.

    - El usuario debe validar el correcto funcionamiento de los equipos al finalizar el mantenimiento. Los usuarios procederán a firmar el reporte que entrega el técnico siempre y cuando el equipo se encuentre en óptimas condiciones.
    - El usuario debe notificar a la OTI o a la mesa de servicios tecnológicos en caso de presentar inconformidad o daño de los elementos o el servicio.

11. Es responsabilidad de los usuarios proteger la información, herramientas y sistemas de información a su cargo para minimizar el riesgo de exposición de la información sensible y activos críticos, cumpliendo con los siguientes lineamientos:

    - Configurar las credenciales de acceso en los equipos de cómputo o dispositivos de los usuarios (Usuario y contraseñas que cumplan con los requisitos de seguridad).
    - Actualizar periódicamente las contraseñas, cumpliendo las características según la política de control de Acceso.
    - No escribir contraseñas o información sensible en papeles, post – it o documentos a la vista.
    - No desatender el equipo de cómputo o dispositivo móvil. En este sentido, debe bloquear el equipo de cómputo, cada vez que se retire de su lugar de trabajo.
    - En los equipos de cómputo suministrados por la Entidad, usar exclusivamente software autorizado por la Unidad.
    - No desatender, ni dejar a la vista documentos o información sensible para la Unidad.
    - Mantener bajo llave documentos físicos, dispositivos móviles, unidades de almacenamiento como son (USB, discos duros, discos extraíbles, CD, DVD) cuando estos no se estén usando.
    - Los equipos de cómputo asignados por la Entidad deben tener configurado solo el papel tapiz y el protector institucional de la Unidad.
    - Los usuarios son responsables de la información que es enviada desde su pc, correo electrónico y/o usuarios en los diferentes sistemas de información.

Artículo 11. Política de seguridad de las operaciones. Esta política consiste en la definición de controles de seguridad relacionados con el procesamiento de la información de la Entidad.

Por consiguiente, con relación al dominio A.12 *"seguridad en las operaciones"* del Anexo A de la ISO/IEC 27001:2013, se establece que:

Se debe identificar, planear, probar, valorar y registrar todo cambio en la infraestructura tecnológica y sistemas de información de la Entidad. Esto para asegurar los recursos como: dotación tecnológica, infraestructura y sistemas de información indispensables en la operación.

Se deben implementar controles con el objetivo de reducir los accesos o cambios no autorizados en los ambientes donde se desarrollan los sistemas de información de la entidad y terceros con relación contractual. Para esto se establecen los siguientes lineamientos:

1. La OTI es responsable de planificar y controlar los cambios relacionados con el mantenimiento o ajuste de los procedimientos, la infraestructura y los sistemas de información que se encuentran a su cargo de manera segura, garantizando la confidencialidad, disponibilidad e integridad de los activos de información; esto mismo aplica para los demás grupos que ejercen desarrollo de sistemas de información dentro de la Entidad.

2. Los usuarios no deben realizar cambios en los equipos de cómputo de trabajo a nivel hardware y/o software relacionado con la configuración del equipo. Estos cambios podrán

ser realizados únicamente por la OTI de la Entidad o por personal autorizado como administrador del equipo de cómputo.

3. La OTI debe proveer la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información.
4. La OTI debe controlar el paso a producción y la administración de los ambientes, que tengan las mismas características técnicas o similares para validar el funcionamiento de las aplicaciones.
5. Todos los cambios planificados se deben realizar por ventana de mantenimiento programada y no afectar los horarios de operación en la entidad.
6. Las herramientas de desarrollo, editores o compiladores no deben tener acceso hacia los ambientes de producción.
7. Los equipos que manejan información de la UARIV deben estar protegidos con antivirus operado por la misma entidad y su actualización automática.
8. La herramienta de control de código malicioso debe realizar análisis de los equipos de cómputo.
9. La OTI podrá hacer seguimiento al tráfico de la red al tener evidencias de actividad inusual o degradación en el desempeño.
10. La OTI debe mantener documentados los presuntos incidentes de seguridad de la información que sean reportados por funcionarios, contratistas y colaboradores de la entidad. De igual manera hacer seguimiento a los eventos inusuales que se presentan y afecten la seguridad de la información o tengan un impacto considerable para el desempeño de los sistemas informáticos.
11. Se prohíbe el uso de software no autorizado por la OTI, en los equipos cómputo proporcionados por la Entidad.
12. La OTI debe llevar a cabo revisiones regulares del software instalado en los equipos de cómputo de la Entidad.
13. Se debe realizar un reporte y recuperación de la información involucrada en ataques con software malicioso.
14. Los directores y jefes de área y/o oficinas, o sus delegados son responsables de gestionar el respaldo de toda la información correspondiente a su respectivo grupo de trabajo, almacenada en equipos de cómputo, en OneDrive o SharePoint.
15. La OTI debe establecer e implementar un plan o protocolo de copias de respaldo para servidores.
16. La OTI debe determinar el plan o protocolo para la restauración de información de servidores.
17. El dominio de infraestructura tecnológica de la OTI de la Unidad debe proporcionar o gestionar el espacio físico y digital para el almacenamiento de copias de seguridad.
18. El dominio de infraestructura tecnológica de la OTI de la entidad debe establecer el ambiente para la restauración de copias de seguridad con el propósito de certificar la calidad de esta.
19. El dominio de infraestructura tecnológica de la OTI de la Unidad debe definir roles y responsabilidades para realizar las actividades de copias de respaldo.
20. El grupo de Gestión Administrativa y Documental de la Unidad es responsable de definir los tiempos para la retención de copias de seguridad e históricos según las tablas de retención documental.
21. La OTI realiza el control y seguimiento (Auditorias Operativas) al proceso de copia de respaldo de la información y restauración.

22. En el marco de sus competencias, los dominios de infraestructura tecnológica y sistemas de información pertenecientes a la OTI deben asegurar la identidad del dispositivo o ubicación y si es posible, el identificador del sistema.
23. Los dominios de infraestructura tecnológica y sistemas de información de la OTI deben registrar intentos de acceso a los sistemas de información que sean exitosos y rechazados.
24. El dominio de infraestructura tecnológica de la OTI es responsable de hacer cambios en la configuración del sistema y uso de privilegios.
25. La OTI es responsable de realizar el monitoreo de las aplicaciones y programas utilitarios del sistema.
26. El dominio de infraestructura tecnológica de la OTI debe tener un inventario sobre direccionamiento y protocolos de red.
27. Los dominios de infraestructura tecnológica y Sistemas de Información de la OTI, deben asegurar que la información de los registros o logs sean protegidos contra toda alteración y acceso no autorizado. Esto mismo aplica para los demás grupos que ejercen desarrollo de sistemas de información dentro de la Entidad.
28. La OTI debe gestionar las vulnerabilidades técnicas de los sistemas de información y adopción de medidas para el control del riesgo.
29. La OTI debe planificar y aplicar las actividades de auditoria a sistemas de información para mitigar el riesgo de interrupción en los procesos de la Unidad.
30. La OTI debe brindar lineamientos a todos los Administradores Funcionales de todas herramientas de la Unidad, para unificar los criterios y manejar una única política interna de administración de usuarios dentro de la entidad.

Artículo 12. Política de seguridad de las comunicaciones. Esta política consiste en la definición e implementación de controles relacionados con el aseguramiento de las redes de comunicaciones y/o servicios de la Entidad.

Por consiguiente, con relación al dominio A.13 *"Seguridad de las comunicaciones"* de la ISO/IEC 27001:2013, se establece que:

1. La OTI debe restringir la conexión de los dispositivos a través del puerto USB, Bluetooth o cualquier otra tecnología inalámbrica
2. La OTI debe restringir los privilegios de administrador a nivel de sistema operativo. (Para equipos asignados por la Unidad o por cualquier operador).
3. Sólo se permite el uso de software licenciado e instalado por personal autorizado a través de la Oficina de Tecnología de la Información para equipos asignados por la UARIV.
4. Los funcionarios, contratistas y colaboradores deben cumplir las políticas, procedimientos y controles para la transferencia de información establecidos por la OTI.
5. Implementar acuerdos de intercambio de información para la transferencia segura de información entre UARIV y las entidades externas.
6. Proteger adecuadamente la información incluida en la mensajería electrónica.
7. La OTI debe implementar las medidas de detección y protección contra el código malicioso que pudiere ser transmitido a través de las comunicaciones electrónicas.
8. La OTI debe controlar el uso de la conectividad inalámbrica.
9. No se permite el acceso a páginas de pornografía, drogas, alcohol, música, concursos en la web, juegos u otras, que no tengan relación con el desempeño de funciones o actividades propias de la UARIV.

10. No se permite descargar, usar, intercambiar y/o instalar (juegos, música, videos, películas, imágenes, protectores, fondos de pantalla, software, información y/o productos) que atenten contra la propiedad intelectual de sus autores o que también contengan (archivos ejecutables, herramientas de hacking y software malicioso) capaces de generar un riesgo de información para la entidad.
11. La entidad puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación de cada usuario desde cualquier puerto y/o protocolo utilizado. Esto como parte de las funciones de administración de la plataforma tecnológica.
12. Los usuarios serán responsables del uso adecuado tanto del internet como de la mensajería interna. En ningún momento aquellos podrán ser utilizados para prácticas ilícitas que atenten contra la entidad, terceros, legislación vigente, políticas o lineamientos de seguridad y privacidad de la información.
13. Los funcionarios, contratistas y colaboradores no podrán asumir en nombre de la entidad posiciones frente a encuestas de opinión, foros, redes sociales u otros medios similares.
14. Los funcionarios, contratistas o colaboradores que hagan parte de redes sociales virtuales como Facebook, Twitter, LinkedIn, Instagram u otros que permitan cualquier tipo de opinión no deberán publicar datos relacionados con la UARIV que no sean avalados y publicados por la Oficina Asesora de Comunicaciones.
15. La mensajería instantánea y el correo electrónico de uso interno o externo deben ser usados exclusivamente en el desempeño de funciones y operatividad de la Entidad.
16. La información, los mensajes y correos electrónicos son propiedad de la Unidad, que está facultada para inspeccionar, registrar y evaluar información intercambiada por estos medios según las funciones de administración de la plataforma tecnológica.

    De acuerdo con el numeral anterior, a continuación, se relacionan los siguientes ítems:

    i. Solo se permite el uso de las herramientas colaborativas de Office 365 autorizadas por la OTI, para mensajería instantánea interna y externa con actividades propias de la Unidad.

    ii. Se prohíbe el uso de cuentas de correo externas (hotmail, gmail, yahoo, etc) o servicios de nube no proporcionados por la Oficina de TI, en la red de la Entidad.

    iii. Los mensajes, equipos de cómputo y la información contenida en buzones de correo corporativo son propiedad de la Unidad.

    iv. No se permite enviar o reenviar cadenas de correo, mensajes con contenidos de carácter corporativo, religioso, político, racista, sexista, pornográfico, publicitario no corporativo u otro tipo que atenten contra la dignidad de las personas, afecten los sistemas internos y de terceros. Tampoco es viable el envío de aquellos que estén en contravía de las leyes, la moral, las buenas costumbres, incitando a prácticas ilícitas o promoviendo a actividades ilegales.

    v. La información sensible de la entidad que requiera ser enviada fuera de sus instalaciones debe seguir los procedimientos de articulación interinstitucional.

    vi. Ningún funcionario, contratista o colaborador no autorizado por la OTI podrá revisar correos electrónicos institucionales de los usuarios o sus correspondientes registros de auditoria. Ello, sin perjuicio de los requerimientos legales y administración de la plataforma tecnológica que se pueda presentar.

    vii. Los usuarios deben evitar el envío de correos electrónicos con información considerada como clasificada o reservada a terceros y/o personal interno.

    viii. Los funcionarios, contratistas y colaboradores son responsables de la información que se envía desde su correo electrónico institucional.

    ix. La OTI debe asignar las medidas, restricciones y controles asociados al reenvió de información sobre medios de comunicación (por ejemplo, el reenvió automático del correo electrónico hacia direcciones externas).

x. La OTI debe realizar la socialización de directrices, políticas y/o buenas prácticas relacionadas con el intercambio de información.

xi. La OTI debe definir estándares técnicos mínimos para la transmisión de la información con entidades externas y procesos de la Entidad.

xii. La OTI define los requisitos de seguridad en la plataforma de correo electrónico para transferencia de información.

xiii. La OTI debe establecer la propiedad y responsabilidad para la protección de datos, derechos de copia conforme con las licencias de software y consideradas similares.

xiv. La OTI y el supervisor del contrato con el proveedor deben socializar, sensibilizar y divulgar las campañas para el buen uso de los sistemas de mensajería electrónica.

xv. La OTI es responsable de identificar, revisar, documentar y actualizar periódicamente los requisitos para los acuerdos de confidencialidad.

Artículo 13. Política de adquisición, desarrollo y mantenimiento de sistemas. Esta política consiste en la implementación de controles en el marco del ciclo de vida del desarrollo de software en la Entidad.

Por consiguiente, con relación al dominio A.14 *"Adquisición, desarrollo y mantenimiento de sistemas"* del Anexo A de la ISO/IEC 27001:2013, la OTI debe realizar la adquisición o desarrollo de software, para su posterior despliegue en ambiente productivo, acorde a los siguientes lineamientos:

1. La OTI debe establecer el plan de trabajo con actividades, responsables, tiempos y fechas de ejecución de los proyectos relacionados con la adquisición, el desarrollo y mantenimiento de software.
2. La OTI debe realizar el levantamiento de las especificaciones funcionales y no funcionales, así como el diseño con mínimo de historial de usuarios y criterios de aceptación.
3. La OTI debe documentar la arquitectura de los sistemas de información que hacen parte de la Entidad.
4. La OTI debe elaborar escenarios de pruebas para garantizar que la solución tecnológica cumpla con los requisitos y necesidades establecidas dentro del marco de seguridad a nivel funcional.
5. La OTI debe ejecutar pruebas unitarias e integrales de la funcionalidad creada o modificada.
6. La OTI debe incorporar los requerimientos de seguridad de la información en la documentación para nuevos desarrollos o nuevas funcionalidades de los sistemas de información.
7. La OTI debe incorporar los requerimientos de seguridad de la información en los sistemas de información que son operados en la actualidad bajo la administración de la Entidad.
8. La OTI debe realizar el análisis, identificación y el correspondiente tratamiento de los riesgos en la fase de diseño a fin de definir los controles de seguridad adecuados.
9. La OTI debe realizar pruebas correspondientes sobre el código fuente de la aplicación.
10. La OTI debe gestionar el Hacking ético periódicamente en las herramientas de producción y/o ambientes controlados.
11. El domino de sistemas de información y/o demás equipos de desarrollo de la Entidad son responsables de verificar que el software puesto en producción haya sido probado en ambiente de pruebas y validado con el usuario final.
12. El dominio de sistemas de información es responsable de implementar la herramienta para el control de las versiones de componentes e ítems de configuración.

13. La OTI debe gestionar los cambios en sistemas de información, con aprobación del propietario o responsable misional de la Información.
14. La OTI debe implementar controles de autenticación para garantizar que el usuario se identifique y en esa medida solo quienes estén autorizados accedan a sistemas de Información.
15. La OTI debe garantizar que las contraseñas se protejan contra modificación, destrucción, copia o divulgación no autorizada mediante almacenamiento cifrado en las bases de datos.
16. La OTI debe implementar controles que determinen el nivel de accesos a la información, menús, parametrización del sistema y demás componentes para que administren los sistemas de Información.
17. La OTI debe generar un log (registros de auditoría) detallado de las actividades que se hacen en el sistema.
18. La OTI debe almacenar el histórico correspondiente a los datos gestionados mediante los sistemas de información de la Entidad.
19. La OTI debe implementar controles en la administración de las fallas en los sistemas de información de la Entidad, generando excepciones controladas cuando se genere un error, evento o incidente.
20. La OTI debe implementar controles que aseguren el funcionamiento de sistemas de información, cuando se realicen actualizaciones o cambios a nivel de sistemas operativos o configuración.
21. La OTI debe realizar validaciones para asegurar la calidad de los datos que son ingresados en sistemas de información evitando ataques de inyección de código.
22. La OTI debe implementar mecanismos de cifrado y control de acceso a la información que sean visibles a los usuarios autorizados.
23. La OTI debe implementar los protocolos seguros (SSL) de cifrado y control de fuga de información.
24. La OTI debe adquirir certificados de sitio seguro para ambientes de producción expuestos en la red pública que aseguren la transmisión de información.
25. La OTI debe asegurar los canales de comunicación para minimizar el riesgo de fuga de información.
26. La OTI debe tener un registro sobre las configuraciones y funcionalidades del sistema que sirva de consulta para la revisión errores del sistema, capacitaciones y transferencias de conocimiento relacionadas con el mismo.
27. La OTI debe usar técnicas de validación de identidad.
28. La OTI debe definir roles y perfiles de usuario para establecer los niveles de acceso asociados a la configuración técnica de los sistemas de información. Los roles y perfiles de los usuarios finales deben ser definidos y gestionados por parte de los administradores funcionales de los sistemas de información.
29. La OTI debe implementar controles para la modificación del código fuente.
30. La OTI debe controlar el número de sesiones por usuario para evitar el uso de credenciales de acceso compartidas.
31. La OTI debe realizar la ofuscación de los datos utilizados en ambientes de prueba.
32. La OTI debe dimensionar la capacidad requerida de la infraestructura que soporte la publicación de sistemas de información en ambiente productivo.
33. La OTI debe controlar el acceso a los ambientes de preproducción y herramientas para el manejo del código fuente.

Parágrafo: Los anteriores lineamentos deben ser aplicados a todos los equipos que realizan desarrollo de software en la Entidad, los cuales deben cumplir los lineamientos de la Oficina de TI.

Artículo 14. Política de relaciones con los proveedores. Esta política consiste en implementación de controles relacionados con el aseguramiento de los productos o servicios suministrados por terceros, que soportan la operación de la Entidad.

Por consiguiente, con relación al domino A.15 *"Relaciones con los proveedores"* del Anexo A de la ISO/IEC 27001:2013, se deben gestionar los riesgos de seguridad de la información asociados con la cadena de suministro, que afecten la continuidad de la operación o servicios de tecnología y comunicación, teniendo en cuenta los siguientes lineamientos:

1. La OTI debe establecer los requisitos de seguridad de la información necesarios para mitigar los riesgos de seguridad de la información asociados con la cadena de suministro que impacten la continuidad de la operación o los servicios de tecnologías y comunicación.
2. La OTI debe llevar a cabo las auditorías de los proveedores y la revisión de reportes respecto a auditorias independientes, además del seguimiento a los hallazgos identificados.
3. La OTI debe gestionar los incidentes de seguridad con proveedores, en el marco de los acuerdos definidos.
4. La OTI debe revisar los aspectos de seguridad de la información de las relaciones de los proveedores con sus terceros.
5. La OTI debe asegurar que el proveedor mantenga una capacidad de servicio suficiente junto con planes ejecutables, para asegurar el mantenimiento de niveles de continuidad del servicio acordados después de fallas considerables en el mismo o luego de un desastre.
6. La OTI debe establecer acuerdos de niveles de servicio con proveedores y entregar informes de seguimiento al cumplimiento.
7. Los proveedores deben reportar a los supervisores, el listado de personal que se ha desvinculado de su compañía para retirar los accesos a servicios y/o información propia de la entidad.
8. Los proveedores de servicios tecnológicos deben garantizar que toda política de seguridad implementada por aquellos cumpla con las políticas y controles de seguridad de la información de la Entidad.

Artículo 15. Política de gestión de incidentes de seguridad de la información. Esta política consiste en la definición de directrices y responsabilidades para garantizar la adecuada gestión de incidentes de seguridad en la Entidad.

Por consiguiente, con relación al dominio A.16 *"Gestión de incidentes de seguridad de la información"* del Anexo A de la ISO/IEC 27001:2013, se establece que:

1. Los usuarios deben reportar eventos y debilidades de seguridad que involucren pérdida, divulgación o modificación no autorizada de información, por medio de la mesa de servicios tecnológicos y canales autorizados:
    - Correo: soporte.oti@unidadvíctimas.gov.co
2. La OTI debe determinar si el evento se considera como incidente de seguridad de la información, según las categorías y criterios de clasificación definidos en los documentos del alcance de procedimiento.
2. La OTI debe atender y clasificar los eventos de seguridad de la información para evaluar y determinar si se ha generado un incidente de seguridad.
3. La OTI debe gestionar los incidentes de seguridad de la información, determinar las lecciones aprendidas y realizar la comunicación a través de los canales adecuados.

4. La OTI debe recolectar la evidencia del incidente y realizar la investigación correspondiente con el fin de determinar las acciones correctivas y preventivas necesarias para mejorar el proceso.

Artículo 16. Política de gestión de la continuidad de negocio. Esta política consiste en la identificación de planes de contingencia y continuidad para actividades y servicios críticos relacionados con la operación.

Por consiguiente, con relación al dominio A.17 del Anexo A "*Aspectos de seguridad de la información de la gestión de continuidad de negocio*" de la ISO/IEC 27001:2013, la Entidad establece que:

1. La OTI en articulación con los procesos estratégicos, misionales y de apoyo debe identificar el grado de criticidad de las actividades y servicios de los procesos que puedan afectar la continuidad de negocio (Análisis de Impacto de Negocio).
2. La OTI en articulación con los procesos estratégicos, misionales y de apoyo debe establecer el plan de contingencia o continuidad del negocio, que cumpla con políticas y controles de seguridad de la Información.
3. La unidad debe identificar los recursos para la obtención de una respuesta efectiva por parte de funcionarios, contratistas y colaboradores en caso de presentarse contingencia o eventos catastróficos que afecten la operación de la entidad.
4. Se debe definir un protocolo de comunicación acorde con las diferentes partes interesadas involucradas.
5. La OTI debe analizar, definir y establecer los requerimientos de redundancia y alta disponibilidad para sistemas de información críticos identificados, acorde al análisis de impacto de negocio. Esto también aplica para los diferentes equipos de desarrollo de la Entidad.
6. La OTI debe evaluar y probar soluciones de redundancia tecnológica implementada para validar los planes de contingencia o continuidad.
7. La OTI debe definir el mecanismo y/o estrategia que cumpla con los requerimientos de alta disponibilidad a nivel de centro de datos, canales de conectividad y sistemas de información.
8. La OTI debe administrar soluciones de redundancia tecnológica y realizar informes sobre dichas soluciones asegurando el cumplimiento de requerimientos de disponibilidad en la entidad.
9. La OTI debe realizar los simulacros de continuidad de negocio definidos para determinar el grado de eficacia y viabilidad del plan, así como hacer revisiones periódicas, para verificar que los controles establecidos sean eficaces en situaciones adversas.

Artículo 17. Política de Cumplimiento. Esta política consiste en la identificación de los requisitos legales, regulatorios, estatutarios o contractuales para el uso adecuado de los activos de información.

Por consiguiente, con relación al dominio A.18 del Anexo A "*Cumplimiento*" de la ISO/IEC 27001:2013, la Entidad establece que:

1. La OTI deberá gestionar el cumplimiento de la legislación correspondiente a seguridad de la información respecto a derechos de autor y propiedad intelectual.
2. Todo software que sea desarrollado y usado en la entidad debe cumplir con los requerimientos legales y de licenciamiento aplicables.
3. La OTI será responsable de mantener el control de todas las licencias de software, hardware y aplicaciones utilizadas por la Entidad.
4. Se prohíbe el uso de software ilegal o no licenciado en la Entidad.

5. La OTI deberá realizar revisiones periódicas a los sistemas de información y estaciones de trabajo.
6. Los funcionarios, contratistas y colaboradores no deben hacer distribución o modificación de software o contener archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la información.
7. Cuando el personal de Servicios TI de la OTI encuentre programas instalados en equipos de cómputo asignados a los usuarios sin el respectivo licenciamiento o autorización, deben desinstalar e informar al dominio de seguridad y privacidad de la información.
8. Todo software, páginas web, documentos, material de contenido gráfico, logos, entre otros que contengan la imagen o el nombre de la Unidad son propiedad de la Entidad, bien sean creados por funcionarios, contratistas y/o colaboradores, en el cumplimiento de sus labores o para el cumplimiento de actividades contractuales propias del contrato según las formalidades del artículo 183 de la ley 23 de 1982 modificado por el art 30 de la ley 1450 de 2011.
9. La Unidad aplica lo establecido en el artículo 183 de la ley 23 de 1982 modificado por el art 30 de la ley 1450 de 2011 y en la decisión andina 351 de 1993, el funcionario, contratista o colaborador es el originario de los derechos morales en desarrollo y ejecución del contrato. En relación con los derechos patrimoniales sobre los productos del contrato pertenecerán a la UARIV.
10. Se autoriza el uso de software libre aprobado por la OTI. En caso de requerir un software libre sin instalación previa, se debe hacer una solicitud dirigida a la – OTI. Esta última llevará un inventario del software de la entidad. La solicitud debe ser realizada a través del correo soporte.oti@unidadvictimas.gov.co.
11. Los sistemas de información adquiridos o desarrollados por terceros deberán contar con un acuerdo de licenciamiento que deberá especificar las condiciones de uso del software y los derechos de propiedad intelectual del mismo.
12. Cuando adquiere un software con un subcontratista, la -OTI- deberá revisar las condiciones contractuales para conocer el alcance, entrega de documentación de arquitectura del sistema de información, del servicio (mantenimiento y soporte), derechos patrimoniales y autorización a modificaciones futuras.
13. Los sistemas de información adquiridos o desarrollados por terceros tienen que contar con un acuerdo de licenciamiento, el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual del mismo.
14. Cualquier software heredado deberá tener la licencia o soporte de transferencia del licenciamiento a la UARIV. En dicha licencia, se deberá indicar si el código transferido a la Entidad es objeto de modificaciones.
15. Para los desarrollos propios de la Entidad se deberá verificar la documentación entregada, artefactos de software y las versiones correspondientes con el fin de ser preservadas en varios medios. Además, deberá guardarse una copia de respaldo externa. La cual deberá registrarse ante la Dirección General de Derechos de Autor.
16. Los funcionarios, contratistas y/o colaboradores responsables de publicar la información en los sitios WEB oficiales de la entidad, deberán atender el cumplimiento de las normas en materia de propiedad intelectual, referente a los derechos de autor y conexos.
17. La Entidad se reserva el derecho a efectuar revisiones del software instalado en equipos de cómputo suministrados por la entidad, en cuanto al licenciamiento requerido.
18. La Entidad establece la política de privacidad y protección de datos personales, de acuerdo con la Ley 1581 de 2012, la cual se debe publicar en la página web oficial.
19. La OTI debe realizar revisiones y auditorías de seguridad a sistemas de información y/o al sistema de gestión de seguridad de la información. Así mismo, debe realizar inspecciones periódicas sobre temas relacionados con seguridad de la información.

Artículo 18: Política y Mesa de Gobierno Digital. La orientación para la implementación de la Política de Gobierno Digital está a cargo del Comité de Gestión Institucional y Desempeño. Sin perjuicio de ello, la Mesa de Gobierno Digital se encargará de articular como de consensuar, las acciones y soluciones relacionadas con la política mencionada para la aprobación posterior por parte del Comité citado conforme a las funciones asignadas a la mesa según la circular Interna No 0036 de 2020.

Artículo 19: El presente acto administrativo rige a partir de la fecha de publicación y deroga en su totalidad la Resolución 740 de 2014.

PUBLÍQUESE Y CÚMPLASE,

Dada en Bogotá D.C. a los

RAMON ALBERTO RODRÍGUEZ ANDRADE
DIRECTOR GENERAL

Aprobación: Victor Edgardo Durán Martínez Jefe Oficina de Tecnologías de la Información
Vladimir Martin Ramos – jefe Oficina Asesora Jurídica
Revisó: Gina Maria Torres. Coordinadora Grupo de Gestión Normativa y Conceptos Oficina Asesora Jurídica
Victoria Eugenia Ibarra Jiménez- Abogada contratista Grupo de Gestión Normativa y Conceptos OAJ
Proyectó: Helena Moreno/Jorge Ramirez /Joaquín Rojas- Oficina de Tecnologías de la Información