Políticas de Seguridad de la Información

Unidad de Tecnologías de Información (UTI)

Dirección de Asuntos Disciplinarios Policiales

DIDADPOL

ENERO 2023

2023 - V 1.0

Acta de Aprobación

Yo, **Silvia Marcela Amaya Escoto**, mayor de edad, soltera, hondureña, abogada, de este domicilio con tarjeta de identidad número 0801-1984-20353, actuando en mi condición de Máxima Autoridad Interina de la Dirección de Asuntos Disciplinarios Policiales (DIDADPOL) nombrada mediante Decreto Ejecutivo No. PCM-056-2021 de fecha 06 de mayo del 2021, con facultades legales suficientes **APRUEBO** las Políticas de Seguridad de la Información de la Unidad de Tecnologías de Información UTI, las cuales consta de los siguientes capítulos:

1. Políticas de Seguridad de la Información
2. Organización de la Seguridad de la Información.
3. Seguridad relativa a los Recursos Humanos
4. Gestión de Activos
5. Control de Acceso
6. Criptografía
7. Seguridad Física y del Entorno
8. Seguridad de las Operaciones
9. Protección contra Software Maliciosos
10. Copias de Respaldo de la Información
11. Registro de Eventos y Monitoreo de los Recursos Tecnológicos y los Sistemas de Información
12. Control al Software Operativo
13. Gestión de Vulnerabilidades
14. Seguridad de las Comunicaciones
15. Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información
16. Relación con Proveedores y Terceras Partes
17. Gestión de incidentes de la seguridad de la información y mejoras
18. Aspectos de Seguridad de la Información para la Gestión de Continuidad de la Institución.
19. Cumplimiento.

E instruyo a todo el personal de la Institución el uso permanente en las funciones que corresponda. Es responsabilidad del encargado de área y su personal el uso permanente y las actualizaciones que correspondan según la ley.

Dado en la ciudad de Tegucigalpa, Municipio del Distrito Central a los veintiséis (26) días del mes de enero del año dos mil veintitrés (2023).

DIRECTOR

Silvia Marcela Amaya
Máxima Autoridad DIDADPOL

Las Políticas de Seguridad de la Información de la Unidad de Tecnologías de Información (UTI) es propiedad de la Dirección de Asuntos Disciplinarios Policiales (DIDADPOL) dependencia desconcentrada de la Secretaría de Estado en el Despacho de Seguridad de Honduras, C.A.

Presidencia de la República de Honduras
Secretaría de Estado en el Despacho de Seguridad
Dirección de Asuntos Disciplinarios Policiales
Unidad de Tecnologías de Información

Elaboración

Unidad de Tecnologías de Información

Revisión Técnica

Unidad de Tecnologías de Información

Centro Cívico Gubernamental (CCG)
José Cecilio del Valle
Torre 1 Piso 19
www.didadpol.gob.hn
Políticas de Seguridad de la Información de la Unidad de Tecnologías de Información
Edición 2023

Actividad	Nombre	Puesto	Firma
Responsable de Elaboración	Ing. Fredis Lagos	Jefe de la Unidad de Tecnologías de Información.	
Responsables de Revisión Técnica	Ing. Luis Fugón Lic. Caleb Rivera Ing. Fredis Lagos	Unidad de Tecnologías de Información	
Responsable de Revisión	Lic. Fabiola Velásquez	Gerente Administrativa Financiera	
Responsable de Aprobación	Abogada Silvia Marcela Amaya	Directora - Máxima Autoridad	

Contenido

GLOSARIO 6
I. INTRODUCCIÓN 10
II. OBJETIVO 11
Objetivos Generales 11
Objetivos específicos 11
1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN. 12
1.1. Compromiso de la Máxima Autoridad. 13
1.2. Sanciones para la violación a las políticas de seguridad de la información 13
1.3. Acuerdo de confidencialidad 13
1.4. Revisión y Comunicación 13
2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. 13
2.1. Estructura organizacional de seguridad de la información 13
2.2. Contacto con Autoridades 14
2.3. Seguridad de la Información en la gestión de proyectos. 15
2.4. Dispositivos Móviles y el Teletrabajo 15
2.4.1. Uso para Dispositivos Móviles 15
2.4.2. Teletrabajo 16
3. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS 17
3.1. Previa a la relación laboral 17
3.2. Durante la relación laboral 18
3.3. Finalización de la relación laboral 19
4. **GESTIÓN DE ACTIVOS** 19
4.1. Responsabilidad de los activos 20
4.1.1. Inventario y propiedad de activos 20
4.1.2. Uso aceptable de los activos 21
4.1.3. Devolución de Activos 23
4.2. Clasificación y manejo de la Información 23
4.2.1. Clasificación de la Información 24
4.2.2. Manejo de Información 24
4.3. Manipulación de Dispositivos de almacenamiento 26

4.3.1. Gestión de Dispositivos de almacenamiento 26
4.3.2. Eliminación de Dispositivos almacenamiento 27
4.3.3. Medios de almacenamiento en transito 27
4.4. Mesa de Ayuda 27
4.5. Compras 28
5. CONTROL DE ACCESOS 28
5.1. Acceso a redes y recursos de red 28
5.2. Gestión de acceso de usuarios 29
5.3. Responsabilidad de acceso de los usuarios 30
5.4. Control de acceso a Sistemas y Aplicaciones 30
6. CRIPTOGRAFÍA 33
6.1. Políticas de uso de los controles criptográficos 34
6.2. Gestión de Claves 34
7. SEGURIDAD FÍSICA Y DEL ENTORNO 35
7.1. Perímetro de Seguridad Física 35
7.2. Seguridad de los equipos 38
8. SEGURIDAD DE LAS OPERACIONES 41
9. PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO (MALWARE) 42
10. COPIAS DE RESPALDOS DE LA INFORMACIÓN 43
11. REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN 44
12. CONTROL AL SOFTWARE OPERATIVO 45
13. GESTIÓN DE VULNERABILIDADES 46
14. SEGURIDAD DE LAS COMUNICACIONES 47
14.1. Gestión y aseguramiento de las redes de datos 47
14.2. Correo Electrónico Institucional 48
14.3. Uso Adecuado De Internet 51
14.4. Intercambio de Información 52
15. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 54
15.1. Requisitos de seguridad en los sistemas de información 54
15.2. Desarrollo y sus Procesos de Soporte. 55
15.3. Datos de Prueba 59
16. RELACION CON PROVEEDORES Y TERCERAS PARTES 59

17. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS .. 61

17.1. Reporte y Tratamiento de Incidentes de Seguridad 61

18. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE LA INSTITUCIÓN 62

18.1. Continuidad de la seguridad de la información 63

18.2. Redundancia 63

19. CUMPLIMIENTO 64

19.1. Cumplimiento de los requisitos legales y contractuales 64

19.2. Revisiones de la seguridad de la información 64

19.3. Privacidad y Protección de Datos Personales 65

GLOSARIO

1. **DIDADPOL:**[1] Dirección de Asuntos Disciplinarios Policiales
2. **Plataformas Tecnológicas:** Es la arquitectura de hardware y software, red de interna y recursos tecnológicos compartidos dentro de la institución que permiten optimizar los procesos y automatizar tareas.
3. **Sistema de Gestión de la seguridad de la información SGSI**[2]**:** consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una Institución, en la búsqueda de proteger sus activos de información esenciales.
4. **ISO:**[3] Organización Internacional de Normalización (ISO)
5. **Norma ISO/IEC 27001:2017**[4]**:** ISO 27001 es una norma desarrollada por ISO (organización internacional de Normalización) con el propósito de ayudar a gestionar la Seguridad de la Información en una institución.
6. **Intranet:** Es una plataforma digital cuyo objetivo es asistir a los funcionarios, empleados, consultores y practicantes, en la generación de valor para la institución, poniendo a su disposición activos como contenidos, archivos, procesos de negocio y herramientas; facilitando la colaboración y comunicación entre las personas y los equipos.
7. **Información pública:** [5]Es toda información que una persona obligado genere, obtenga, adquiera, o controle en su calidad tal y que es determinada por la ley a ser declarada como información pública, no confidencial.
8. **Cifrado:** Un procedimiento utilizado para convertir los datos de su forma original a un formato que sea ilegible o inutilizable a nadie sin la herramientas e información necesaria para invertir el proceso de cifrado.

[1]https://didadpol.gob.hn/sobre-didadpol/
[2] https://www.pronabec.gob.pe/sistema-de-gestion-de-seguridad-de-la-informacion/#:~:text=El%20Sistema%20de%20Gesti%C3%B3n%20de,etc.)%2C%20entre%20otros.
[3]https://www.iso.org/what-we-do.html
[4]https://normaiso27001.es/
[5] http://aprendizaje.iaip.gob.hn/biblioteca/biblioteca/curso/3001/modulo/3003/

9. **Confidencialidad:** [6]Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
10. **Recursos tecnológicos:** Son aquellos activos de hardware y software tales como: servidores (de aplicaciones y de servicios de red), computadoras, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la institución.
11. **Puerto USB:**[7] El término se emplea para nombrar a una clase de conexión que posibilita el envío y la recepción de información. USB, por su parte, es la sigla correspondiente a Universal Serial Bus, una interfaz que permite la conexión de periféricos a diversos dispositivos, entre los cuales se encuentran los ordenadores y los teléfonos móviles.
12. **Correo Electrónico Institucional:** [8]Sistema mediante el cual un ordenador puede intercambiar mensajes con otros usuarios de ordenadores (o grupos de usuarios) mediante redes de comunicación.
13. **Sistemas de Información:** [9]Un Sistema de Información (SI) es un conjunto de componentes interrelacionados que trabajan juntos para recopilar, procesar, almacenar y difundir información para apoyar la toma de decisiones. Además, apoyan la coordinación, control, análisis y visualización de una organización.
14. **Consultor[10]:** Todas las personas naturales, nacional o internacional que se centran en la optimización de las prácticas de operaciones de la Institución y pueden asesorar sobre métodos o técnicas de operaciones más eficientes.
15. **Terceras Partes:** Entidades judiciales, demás entes del Estado de la Republica de Honduras y Cooperantes internacionales.

[6] http://definicion.de/confidencialidad/
[7] https://definicion.de/puerto-usb/
[8] https://www.glosarioit.com/Correo_electr%C3%B3nico
[9] https://www.kionetworks.com/blog/data-center/los-sistemas-de-informacion-de-una-empresa#:~:text=Un%20Sistema%20de%20Informaci%C3%B3n%20(SI,y%20visualizaci%C3%B3n%20de%20una%20organizaci%C3%B3n.
[10] https://historiadelaempresa.com/consultores-externos-vs-internos#:~:text=Los%20consultores%20externos%20trabajan%20para,a%20largo%20plazo%20y%20continua.

16. **Proveedor:** Todas las personas, jurídicas o naturales, como, contratistas, que provean servicios o productos a la DIDADPOL, los cuales son necesarios para su desarrollo y funcionamiento.
17. **Propietario de la información**[11]**:** El propietario de la información es la persona responsable de la integridad, confidencialidad y disponibilidad de una cierta información.
18. **Funcionario**[12]: es aquella persona que presta sus servicios a la Administración Pública y bajo juramentación de la Máxima Autoridad.
19. **VPN:**[13] "Virtual Private Network" (Red privada virtual) y describe la oportunidad de establecer una conexión protegida al utilizar redes públicas.
20. **Clave:** [14]Es una combinación de caracteres (letras, números y signos), que debe teclearse para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc.
21. **Firmware:** Este software puede ser capaz de proporcionar un entorno de operación para las funciones más complejas del componente, o bien puede actuar como el propio sistema operativo interno del componente.
22. **Hacking ético**: [15]Es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.
23. **Malware:** Software de intención e impacto malicioso, como virus, gusanos, y software espía.
24. **Ataque**: Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo.

---

[11] http://wiki.derechofacil.gob.ar/index.php/Propietario_de_la_informaci%C3%B3n#:~:text=El%20propietario%20de%20la%20informaci%C3%B3n,disponibilidad%20de%20una%20cierta%20informaci%C3%B3n.
[12] https://economipedia.com/definiciones/funcionario-publico.html
[13] https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn
[14] https://www.glosarioit.com/Clave_de_acceso
[15] https://hacking-etico.com/

25. **Registros de Auditoría:** Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, equipos tecnológicos y redes de datos de la institución. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.
26. **Entidad Gubernamental:** [16] es aquella que provee un servicio público a la ciudadanía. Su gestión suele estar a cargo del Gobierno en funciones, aunque en algunos casos se le brinda cierta autonomía nombrando a gestores independientes al mando de la institución.

[16] https://economipedia.com/definiciones/entidad-gubernamental.html#:~:text=Una%20entidad%20gubernamental%20es%20aquella,al%20mando%20de%20la%20instituci%C3%B3n.

I. INTRODUCCIÓN

La información y la plataforma tecnológica, son activos importantes y vitales de la Dirección de Asuntos Disciplinarios Policiales DIDADPOL, es por eso que las Políticas de Seguridad de la Información constituyen parte fundamental para la implementación de un Sistema de Gestión de Seguridad de la Información de la DIDADPOL.

Las siguientes Políticas de la Seguridad de la Información son una serie de normas y directrices basadas en la Norma internacional ISO/IEC 27001:2017 y sus debidas recomendaciones que describe requisitos para la gestión y controles de la seguridad de la Información, las cuales serán actualizadas cuando lo amerite, acoplándose a la estructura de la Institución.

Las políticas incluidas constituyen como parte fundamental del Sistema de Gestión de Seguridad de la Información de la DIDADPOL, y se convierten en la base para la implementación de las sanciones definidas. La seguridad de la información es una prioridad para la DIDADPOL y por tanto es responsabilidad de todos velar porque no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

Las Políticas de Seguridad de la Información resguardan los aspectos administrativos y de control que deben ser cumplidos por todos los funcionarios, empleados, consultores y practicantes de la DIDADPOL, proveedores y terceras partes para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

Las violaciones a los lineamientos y negligencias en el cumplimiento de lo establecido en estas políticas pueden resultar en acciones disciplinarias de acuerdo a las normativas establecidas por el Reglamento De Organización y Funciones de la DIDADPOL o acuerdo de confidencialidad de la DIDADPOL, las cuales son de conocimiento de todos los funcionarios, empleados, consultores y practicantes de la institución.

II. OBJETIVO

Objetivos Generales

Determinar las normas y directrices de cumplimiento obligatorio de los distintos componentes de las Políticas de Seguridad de la Información. Esto con la finalidad de proteger el principal activo de la DIDADPOL que es la información, asegurando así la confidencialidad, integridad y disponibilidad de la misma y de los Sistemas de Información, manteniendo la información oportuna y verificable para la toma de decisiones.

Objetivos específicos

1. Establecer normas y directrices para la protección de activos y recursos de la información para garantizar que solo usuarios autorizados puedan tener acceso a información de la DIDADPOL, evitando posibles riesgos y ataques.

2. Definir normas para la gestión de activos, acceso a las plataformas tecnológicas, sistemas de información, aplicaciones, envió y recepción de información, que permita crear vínculos seguros con integridad, disponibilidad y confidencialidad de la información.

3. Determinar las políticas de seguridad para los controles de acceso a la información, estableciendo los niveles de permisos de acceso a redes de datos y controles físicos en la DIDADPOL.

1. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

La Política de Seguridad de la Información de la DIDADPOL se encuentra fundamentada por políticas, normas y procedimientos específicos en los dominios y objetivos de control de la norma internacional ISO 27001:2017 Anexo A, los cuales guiarán el manejo adecuado de la información de la institución.

Esta política ayudara a los funcionarios, empleados, consultores y practicantes de la DIDADPOL, proveedores y terceras partes a determinar qué información es confidencial o compartida, así como la sensibilidad de la información que no debe ser revelada o compartida fuera o dentro de la DIDADPOL sin la debida autorización.

La información amparada en la presente política incluye información que es almacenada o compartida a través de cualquier medio. Esto incluye: información digital, información sobre el papel y la información compartida vía oral o visualmente (por ejemplo, audio, fotografías y vídeo).

Toda la información de la DIDADPOL se clasifica en dos categorías principales:

- Información Pública de la DIDADPOL
- Información Confidencial de la DIDADPOL

Información pública de la DIDADPOL es la información que ha sido declarada en conocimiento público y publicada en nuestra página oficial de la institución https://didadpol.gob.hn/, redes sociales oficiales, portales de Transparencia del Instituto de Acceso a la Información Pública que pueden darse libremente a cualquier persona sin ningún daño posible a la DIDADPOL.

Información Confidencial de la DIDADPOL es la información que ha sido declarada en conocimiento privada y reservada, es toda la información mencionada en la cuarta cláusula del acuerdo de confidencialidad de la DIDADPOL.

1.1. Compromiso de la Máxima Autoridad.

La Máxima Autoridad aprueba esta Política de Seguridad de la Información como muestra de su responsabilidad en el diseño e implementación de políticas eficientes que certifiquen la seguridad de la información en la DIDADPOL.

1.2. Sanciones para la violación a las políticas de seguridad de la información

Las Políticas de la Seguridad de la Información procuran mantener una cultura de seguridad de la información dentro de la DIDADPOL, sujeta al Reglamento de Organización y Funciones de la Dirección de Asuntos Disciplinarios Policiales DIDADPOL por incumplimiento de políticas de Seguridad de la Información.

1.3. Acuerdo de confidencialidad

Todo funcionario, empleado, consultor, practicantes, proveedor y terceras partes deberán firmar acuerdo de confidencialidad sobre el manejo y uso de información antes de empezar una relación laboral con la DIDADPOL.

1.4. Revisión y Comunicación

Las políticas de seguridad deben ser publicadas en la Intranet de la Institución DIDADPOL para acceso de todos los funcionarios, empleados, consultores, practicantes, proveedores y terceras partes, siendo socializadas al personal mínimo una vez al año o cuando existan cambios sustanciales en la Institución.

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

La DIDADPOL definirá roles, perfiles, funciones y responsabilidades que se consideren actividades de administración, operación y gestión de la seguridad de la información.

2.1. Estructura organizacional de seguridad de la información

a. La Máxima Autoridad de la Institución debe examinar y aprobar las Políticas de la Seguridad de la Información contenidas en este documento.

b. La Máxima Autoridad deberá promover la divulgación y socialización de las políticas de Seguridad de la Información a todos los funcionarios, empleados, consultores y practicantes de la Institución.

c. La Máxima Autoridad debe impulsar una cultura de seguridad de la información en la Institución.

d. La Máxima Autoridad debe asegurar el fortalecimiento de los recursos correctos para la implementación de las Políticas de Seguridad de la Información

e. Los Gerentes de áreas y jefes de Unidades deben participar activamente para cumplir con las Políticas de Seguridad de la Información.

f. La Gerencia de Administración Financiera debe estipular los recursos, la infraestructura física y personal necesario para la gestión de la seguridad de la información de la institución.

g. La Unidad de Tecnologías de Información UTI debe establecer controles, funciones, roles y responsabilidades a los funcionarios, empleados, consultores y practicantes de la DIDADPOL, proveedores y terceras partes para la gestión de las plataformas tecnológicas y sistemas de información de la institución.

h. Los funcionarios, empleados, consultores y practicantes de la DIDADPOL, proveedores y terceras partes tienen la responsabilidad de cumplir con las normas y políticas, procedimientos y estándares referentes a la seguridad de la información.

2.2. Contacto con Autoridades

a. La Gerencia Administrativa Financiera debe manejar registro de contactos de cuerpos de seguridad del estado y servicios de emergencia en caso de incidentes.

b. La Unidad de Tecnologías de Información UTI debe manejar registro de contactos de proveedores y entes del estado que le permitan acudir en casos de incidentes de seguridad de la información.

2.3. Seguridad de la Información en la gestión de proyectos.

a. La Dirección, Gerencias y Unidades de la DIDADPOL deberán involucrar en todos los proyectos las Políticas de Seguridad de la Información, independiente del tipo de proyecto.

2.4. Dispositivos Móviles y el Teletrabajo

2.4.1. Uso para Dispositivos Móviles

a. Los funcionarios, empleados, consultores y practicantes deben resguardar la información que manejen fuera de las Instalaciones de la DIDADPOL de acuerdo con las normas y políticas, procedimientos y estándares referentes a la seguridad de la información.

b. Los funcionarios, empleados, consultores y practicantes que requieran retirar de las oficinas de la DIDADPOL dispositivos móviles como ser laptop, proyectores, cámaras etc. asignados de manera temporal., Debe previamente informar sobre la salida de dicho equipo a la Unidad de Bienes donde llenara el formato correspondiente. En caso de las oficinas regionales dicho proceso se realizará con el enlace administrativo.

c. Todos los dispositivos móviles como laptop, celulares, tablet o cualquier otro de esta índole propiedad de la DIDADPOL y asignado los funcionarios, empleados, consultores y practicantes, debe contar con un sistema de bloqueo alfanumérico (no patrones gráficos), cuya contraseña será conocida por el administrador del dispositivo y por la Unidad de Tecnologías de Información UTI.

d. En caso de pérdida o robo del equipo tecnológico los funcionarios, empleados, consultores y practicantes deben notificar en la brevedad posible a la Unidad de Bienes para realizar el debido proceso correspondiente, apegado a las políticas de Bienes Nacionales.

2.4.2. Teletrabajo

a. La Unidad de Tecnologías de Información UTI, deben analizar y aprobar los métodos de conexión remota a la plataforma tecnológica y sistemas de información de la DIDADPOL.

b. La Unidad de Tecnologías de Información UTI debe implementar los métodos y controles de seguridad para establecer conexiones remotas segura hacia la plataforma tecnológica y sistemas de información de la DIDADPOL.

c. La Unidad de Tecnologías de Información UTI debe restringir las conexiones remotas a los recursos de la plataforma tecnológica y sistemas de información; únicamente se deben permitir estos accesos a los funcionarios, empleados, consultores y practicantes autorizados de la de DIDADPOL, por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

d. La Unidad de Tecnologías de Información UTI debe asegurar que toda computadora portátil o disco externo de almacenamiento de la Institución tenga instalado un sistema de cifrado en su disco duro, para salvaguardar la información en caso de pérdida o robo del equipo.

e. La Unidad de Tecnologías de Información UTI bloqueara los puertos USB de los equipos tecnológicos, con el fin de evitar riesgos de vulnerabilidades y garantizando la seguridad de la información. Procurando así que los funcionarios, empleados, consultores y practicantes solo utilicen medios de almacenamiento establecidos por Unidad de Tecnologías de Información UTI. Serán habilitados estrictamente en casos que sus funciones laborales lo requieran.

f. La Unidad de Tecnologías de Información UTI deberá instalar en las computadoras que estén en teletrabajo un software de respaldo automatizado, asegurando la información que se maneja en dicho equipo sea respaldada.

g. La Unidad de Tecnologías de Información UTI debe dar prioridad para que los funcionarios, empleados, consultores y practicantes utilicen computadora propiedad de DIDADPOL, en caso que no se pueda, el usuario podrá usar su computadora personal, siempre y cuando sea previamente revisada por el personal técnico de la Unidad de Tecnologías de Información UTI, validando que dicho equipo tenga antivirus actualizado y actualizaciones al día de su sistema operativo.

h. Los funcionarios, empleados, consultores y practicantes únicamente deben establecer conexiones remotas a la red interna en computadores propiedad de DIDADPOL o previamente identificadas por la Unidad de Tecnologías de Información UTI y, bajo ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.

i. Los funcionarios, empleados, consultores y practicantes son responsable del cuidado físico de cualquier equipo tecnológico asignado al momento de ser traslado fuera de las oficinas de la DIDAPDOL.

3. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

Esta política reconoce la intervención de la Unidad de Recursos Humanos para cumplir con los objetivos de la misma.

3.1. Previa a la relación laboral

La política tiene como interés de contar con el personal mejor calificado, permitiendo garantizar que la vinculación del nuevo personal se realice siguiendo un proceso formal de selección, acorde a los procedimientos establecidos, el cual estará orientado a las funciones y roles que se desempeñan en sus cargos.

a. La Unidad de Recursos Humanos debe realizar verificaciones de acuerdo a las leyes, normativa y códigos éticos que sean de aplicación y proporcionales a las necesidades de la institución y que a su vez permitan validar la información suministrada por los candidatos a ocupar un puesto en la DIDADPOL.

b. La Unidad de Recursos Humanos debe certificar que los funcionarios, empleados, consultores y practicantes que firmen acuerdo de confidencialidad, el cual establecerá sus obligaciones en institución para la seguridad de información, y será adjuntado a su expediente.

c. Los proveedores que realicen labores para la DIDADPOL, deberán firmar un Acuerdo de Confidencialidad y documentos de aceptación de Políticas de Seguridad de la Información, antes de conceder acceso a las instalaciones o plataformas tecnológicas de la DIDADPOL, realizado por la Gerencia Administrativa Financiera, el cual debe archivar dicho proceso.

3.2. Durante la relación laboral

La política tiene el fin de salvaguardar la información procurando que el personal cuente con los conocimientos deseados en seguridad de la información para una correcta gestión de los activos de información en la DIDADPOL.

a. La Unidad de Tecnologías de Información UTI debe capacitar periódicamente a los funcionarios, empleados, consultores y practicantes sobre las Políticas de Seguridad de la Información de la Institución.

b. Los funcionarios y empleados que incumplan con las Políticas de Seguridad de la Información conllevaran a la aplicación establecida en el Reglamento de Organización y funciones de la DIDADPOL.

c. Todos los funcionarios, empleados, consultores y practicantes recibirán una inducción del uso adecuado del equipo tecnológico, uso de sistemas de información, aplicaciones, plataformas tecnológicas y correo electrónico por parte de la Unidad de Tecnologías de Información UTI al momento de entregarle su equipo tecnológico asignado.

d. Los consultores y practicantes que incumplan con las Políticas de Seguridad de la información conllevaran quitar relación alguna con la institución DIDADPOL.

3.3. Finalización de la relación laboral

La política asegurará que el personal será desvinculados o reasignado para nuevo puesto de una forma ordenada, controlada y segura.

a. La Unidad de Recursos Humanos debe comunicar anticipadamente la finalización laboral, licencias, vacaciones o cambios de labores de los funcionarios, empleados, consultores y practicantes a la Unidad de Tecnologías de Información UTI para realizar los procedimientos y controles establecidos correspondientes.

b. La Unidad de Bienes es responsable de hacer el respectivo descargo de los bienes tecnológicos en acompañamiento de un técnico de la Unidad de Tecnologías de Información UTI, validando que el equipo se encuentre en buenas condiciones. Los equipos tecnológicos pasaran posteriormente a la custodia de la Unidad de Bienes.

c. La obligación de confidencialidad establecida por esta política, a los funcionarios, empleados, consultores, practicantes, proveedores de la DIDADPOL y terceras partes se extiende a 4 años después del período de cese de empleo o relación de servicios.

4. GESTIÓN DE ACTIVOS

La DIDADPOL como propietaria de los activos físicos, información generada, almacenada, procesada por su plataforma tecnológica y sistemas de información, otorga responsabilidad a la dirección, las gerencias y jefaturas sobre sus activos de información, asegurando se cumplan las directrices que se mencionan en esta política.

La información, archivos físicos, los sistemas de información, los servicios y los equipos tecnológicos (ej. computadoras, fotocopiadoras, impresoras, redes, internet, correo electrónico institucional, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) propiedad de la DIDADPOL, son activos de la institución y se proporcionan a los

funcionarios, empleados, consultores y practicantes, para cumplir con los propósitos de la institución.

4.1. Responsabilidad de los activos

4.1.1. Inventario y propiedad de activos

a. La Máxima Autoridad, los gerentes y jefes propietarios de la información electrónica de su área, tendrán la facultad de aprobar o revocar el acceso a su información de su gerencia y unidad al personal que requieran. Dicha aprobación o revocación deberán realizarla previamente vía correo electrónico institucional u otro medio que se designe por la Unidad de Tecnologías de Información UTI.

b. La Unidad de Tecnologías de Información UTI debe monitorear periódicamente la validez operacional de los recursos tecnológicos y sus perfiles de acceso a la información.

c. La DIDADPOL es la propietaria de los activos de información correspondientes a las plataformas tecnológicas y sistemas de información, la cual es administrada por la Unidad de Tecnologías de Información UTI, en consecuencia, debe asegurar su apropiada operación.

d. Todo equipo tecnológico entregado por la Unidad de Bienes, debe estar asignado a un funcionario o empleado, el cual será responsable del uso debido y su cuidado; deberán firmar la Ficha de Asignación, la cual describe los bienes. En caso de consultores y practicantes la asignación del equipo tecnológico se realizará al jefe inmediato.

e. El Inventario y asignación de equipo tecnológico propiedad de la DIDADPOL es responsabilidad de la Unidad de Bienes. Dicha asignación se realizará con recomendación técnica de la Unidad de Tecnologías de Información UTI dependiendo de las funciones que realice dicho funcionario, empleado, consultor y practicante.

f. La Unidad de Bienes es responsable de recibir los equipos tecnológicos para su reasignación o disposición final y la Unidad de Tecnologías de Información UTI de generar copias de seguridad de la información de los funcionarios, empleados, consultores y practicantes que se retiran o cambian de labores, cuando les es formalmente solicitado, creando un archivo digital histórico.

g. Las fotografías, audios, videos y documentos generados durante la ejecución del trabajo serán para el uso y propiedad exclusiva de la DIDADPOL. Los funcionarios, empleados, consultores y practicantes deben ser consciente que los recursos de procesamiento de información están sujetos a auditorias.

h. La información recibida directa o indirectamente por los funcionarios, empleados, consultores y practicantes acerca de las operaciones de la DIDADPOL, relacionada a denuncias, investigación, expedientes, casos legales, y temas relacionados, se considera sensible y confidencial, y no podrán ser reveladas a personas ajenas a la Institución, ni ser discutidas fuera del ámbito de laboral excepto cuando sea apropiado y necesario dentro del curso de las operaciones de la DIDADPOL.

i. Debido a que los funcionarios, empleados, consultores, practicantes y proveedores podrían tener acceso a información sensible y confidencial, cualquier información que compartan en relación a su experiencia profesional con la institución, debe ser aprobada previamente por el gerente del área y la máxima autoridad de la DIDADPOL; ningún documento digital o impreso podrán ser retirados de las oficinas excepto con autorización escrita por el gerente del área o máximas autoridades de la DIDADPOL.

4.1.2. Uso aceptable de los activos

a. La Unidad de Tecnologías de Información UTI debe establecer una configuración aceptable para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

b. La Unidad de Tecnologías de Información UTI es responsable de preparar el equipo tecnológico de los funcionarios, empleados, consultores y practicantes, y de hacer entrega de las mismas en acompañamiento del oficial de Bienes.

c. La Unidad de Tecnologías de Información UTI deberá proveer protocolos de seguridad como contraseñas, métodos de cifrado para almacenar información digital confidencial.

d. Los funcionarios, empleados, consultores y practicantes deben mantener alejado comidas y bebidas del entorno donde está colocado el equipo tecnológico, evitando así se vea afectado el equipo por cualquier derramamiento.

e. Los funcionarios, empleados, consultores y practicantes solo deben utilizar software con licenciamiento original y únicamente la Unidad de Tecnologías de Información UTI está autorizado a realizar dicha instalación.

f. Los funcionarios, empleados, consultores y practicantes no deben solicitar a la Unidad de Tecnologías de Información UTI la instalación de software en sus computadoras asignadas por la DIDADPOL para realizar actividades personales.

g. Los funcionarios, empleados, consultores y practicantes deben darle un uso adecuado al equipo tecnológico asignado, tomando en cuenta el cuidado del mismo y evitando conectar accesorios no necesarios para las funciones laborales.

h. Los funcionarios, empleados, consultores y practicantes deben reportar inmediatamente a la Unidad de Tecnologías de Información UTI, cualquier falla que afecte la integridad y funcionamiento del equipo asignado, evitando hacer cualquier tipo de manipulación del equipo tecnológico.

i. Los funcionarios, empleados, consultores y practicantes no deben conectar computadoras o dispositivos tecnológicos personales o de terceros a la red cableada local de la DIDADPOL.

j. Para cualquier otro propósito diferente a las funciones de la DIDADPOL, los funcionarios, empleados, consultores y practicantes, incluyendo terceras partes que colaboren con la institución, deberán pedir previa autorización para el uso de información antes de ser distribuido de cualquier forma al público en general (medios de comunicación, redes sociales, familia, amigos etc.), dicho permiso debe ser aprobado por la Máxima Autoridad de la DIDADPOL.

k. La información personal de contacto y su localización de los funcionarios, empleados, consultores y practicantes de la DIDADPOL solo podrá ser distribuida con previa autorización de la Unidad de Recursos Humanos.

l. Los funcionarios, empleados, consultores, practicantes y proveedores que posean información almacenada de la DIDADPOL en cualquier dispositivo tecnológicos deben mantenérsela fuera de acceso y vista de personas no autorizadas.

4.1.3. Devolución de Activos

a. En el momento de finalización laboral, los funcionarios, empleados, consultores y practicantes deben realizar la entrega del equipo tecnológico asignado al oficial de Unidad de Bienes en acompañamiento de oficial de la Unidad de Tecnologías de Información UTI.

b. En el momento de cambio de puesto, los funcionarios, empleados, consultores y practicantes mantendrán su equipo tecnológico asignado o se le reasignara otro equipo tecnológico según las funciones labores que vaya a ejercer, según lo establecido en la sección 4.1.1 inciso b.

4.2. Clasificación y manejo de la Información

La DIDADPOL definirá niveles más adecuados para la clasificación de la información de acuerdo con su sensibilidad y generará una guía de clasificación de información para

que los funcionarios, empleados, consultores y practicantes puedan catalogarla y determinen los controles requeridos para su protección.

La Unidad de Tecnologías de información UTI proporcionara los recursos necesarios para la aplicación de los controles en busca de almacenar y preservar la confidencialidad, integridad y disponibilidad de la información. Promoviendo el uso adecuado por parte del personal de la institución, evitando que tercero no autorizados tenga acceso a la misma.

4.2.1. Clasificación de la Información

Esta política permitirá garantizar que la información reciba un nivel adecuado de protección de acuerdo a su importancia dentro de la institución.

a. La Unidad de Tecnologías de Información UTI debe clasificar toda la información generada por la Institución, aplicando los respectivos privilegios de acceso.

b. Los funcionarios, empleados, consultores y practicantes que manejen información, deben clasificar su información de acuerdo con la guía de la clasificación de Información establecida. También monitorear periódicamente su clasificación y realizar cambios de reclasificación de ser necesario.

4.2.2. Manejo de Información

a. La Dirección, Gerencias y Unidades solo podrán realizar destrucción de información física cuando se han cumplido su ciclo de 10 años almacenados, asegurándose anticipadamente de mantener dicha información de manera digital.

b. La Dirección, Gerencias y Unidades debe utilizar el protocolo establecido para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma, aplicando los registros correspondientes sobre qué información física se esta destruyendo.

c. La Unidad de Tecnologías de Información UTI debe proveer los métodos de cifrado de la información, y administrar el software o herramienta utilizado para tal fin.

d. La Unidad de Tecnologías de Información de UTI capacitará a los funcionarios, empleados, consultores y practicantes de la DIDADPOL al momento de entregar su equipo tecnológico, acerca del protocolo de cifrado a seguir en el envío y lectura de correos electrónicos.

e. La Unidad de Tecnologías de Información UTI debe utilizar métodos de borrado seguro de la información, cuando se realiza bajas de equipos tecnológicos.

f. Los oficiales de denuncias, investigadores y técnicos legales que reciban medios de prueba digital, deberán grabarlos en CD-DVD y rotularlo con número de expedientes y folio para añadirlos a los folios de sus expedientes correspondientes.

g. La Unidad de Tecnologías de Información creara manuales y capacitara a los oficiales de recepción de denuncias, investigadores y técnicos legales en procesos de grabación de información en medios de almacenamiento CD, DVD, USB etc.

h. Los oficiales de recepción de denuncias, investigadores y técnicos legales que necesiten realizar procesos de recolección de medios de pruebas digitales dentro de la Institución y requieran respaldo para extracción de medios de pruebas digitales en dispositivos de almacenamiento complejos, podrán solicitar apoyo a la Unidad de Tecnologías de Información para el asesoramiento del mismo.

i. Los investigadores y técnicos legales que necesiten realizar procesos de identificación, recolección, adquisición y preservación de medios de pruebas digitales complejas en dispositivos pertenecientes a la Secretaria de Estado en el Despacho de Seguridad y Policía Nacional de Honduras podrán solicitar

colaboración a la Dirección Policial de Telemática con la participación del personal operativo de la DIDADPOL en dichas diligencias. Recordando que la DIDADPOL puede realizar a nivel nacional y dentro del plazo de investigación establecido la verificación e inspección de información contenidas en celulares, computadores, cámaras de seguridad, grabaciones de audio y vídeo, publicaciones en portales electrónicos o páginas web; propiedad de la institución (artículo 77, numeral 5 REGLAMENTO DISCIPLINARIO APLICABLE AL PERSONAL DE LA SECRETARÍA DE ESTADO EN EL DESPACHO DE SEGURIDAD Y MIEMBRO).

j. L Los investigadores que necesiten realizar procesos de recolección, extracción e inspección de medios de pruebas digitales en entidades públicas o privadas distintas a la Secretaria de Estado en el Despacho de Seguridad y Policía Nacional de Honduras deberán solicitar autorización por escrito al encargado del área , acompañando dicha recolección, extracción e inspección por personal operativo de la DIDADPOL . La Unidad de Tecnología de Información de la DIDADPOL podrá asesorar al investigador para la recolección de la misma en caso de ser necesario.

k. La unidad de Comunicaciones deberá grabar sus medios de pruebas digitales encontrados en medios de comunicación, redes sociales o cualquier otro medio de comunicación en CD o DVD.

4.3. Manipulación de Dispositivos de almacenamiento

Esta política ayudara a prevenir la divulgación, modificación, retiro o destrucción no autorizada de la información almacenada en los medios de almacenamiento.

4.3.1. Gestión de Dispositivos de almacenamiento

a. Los equipos tecnológicos mantendrán una política de bloqueos de puertos USB. En caso que los funcionarios, empleados, consultores y practicantes necesiten acceso a los mismos deben solicitar vía correo electrónico a la Unidad de

Tecnologías de Información UTI, la cual evaluara dicha solicitud, teniendo como prioridad la seguridad de información de la DIDADPOL.

b. Para la transferencia de archivos los funcionarios, empleados, consultores y practicantes deben usar las carpetas compartidas de la red local o correo electrónico institucional de la DIDAPDOL. La Unidad de Tecnologías de Información UTI es responsable de administrar y dar los privilegios correspondientes, con previa autorización de los gerentes de áreas y jefes de unidades.

4.3.2. Eliminación de Dispositivos almacenamiento

a. La Unidad de Tecnologías de Información UTI deben implementar un sistema de borrado seguro en los dispositivos tecnológicos que serán dados de baja de la Institución.

4.3.3. Medios de almacenamiento en transito

a. La DIDADPOL debe concientizar a todos los funcionarios, empleados, consultores y practicantes de la institución en la responsabilidad del manejo de información física y digital en tránsito, asegurándose el acceso no autorizado y mal uso durante el transporte del mismo.

b. Los funcionarios, empleados, consultores y practicantes deben cumplir con el proceso establecido por la Unidad de Tecnologías de Información UTI sobre el tránsito de medios de almacenamiento o información física de la Institución.

4.4. Mesa de Ayuda

a. Cada solicitud o soporte técnico realizado a la Unidad de Tecnologías de Información debe realizarse por el medio el Sistema de Tickets que está a disposición en las computadoras de cada funcionario, empleado, consultor y practicante la Institución. En el caso que su computadora no funcione para realizar dicha solicitud, podrá hacerlo vía llamada telefónica a la Unidad, con el

compromiso de que cuando su solicitud sea resuelta deberá llenar el respectivo ticket

4.5. Compras

a. La Unidad de Tecnologías de Información UTI debe analizar las necesidades tecnológicas de la Dirección, gerencias y unidades, proponiendo a la Gerencia Administrativa las necesidades de compras de equipo tecnológicas, generando anticipadamente un requerimiento técnico por cada compra.

5. CONTROL DE ACCESOS

5.1. Acceso a redes y recursos de red

La Unidad de Tecnologías de Información UTI es la responsable de las redes de datos y los recursos de red, asegurando a través de mecanismos de control que dichas redes estén debidamente protegidas contra accesos no autorizados, proporcionando acceso a las redes y a los servicios en red para cuyo uso hayan sido específicamente creadas.

a. La Unidad de Tecnologías de Información UTI debe establecer procedimientos de autorización y controles de acceso a la red de datos y recursos de la DIDADPOL.

b. La Unidad de Tecnologías de Información UTI debe asegurar que las redes inalámbricas de la institución cuenten con métodos de autenticación que evite accesos no autorizados.

c. La red inalámbrica de la DIDADPOL que es usada por visitantes debe estar aislada de la red local principal, dicho acceso será controlado y queda a discreción de la Unidad de Tecnologías de Información UTI, limitar o restringir el mismo.

d. Los funcionarios, empleados, consultores, practicantes, proveedores y terceras partes no deben descargar ningún tipo de archivos de fuentes no autorizadas,

desconocidas o sospechosos. Evitando alguna vulnerabilidad que ponga en riesgo la seguridad y funcionalidad de los sistemas de información, red interna y equipo tecnológico. En caso de ser estrictamente necesario por temas laborales deberán abocarse a la Unidad de Tecnologías de Información UTI para realizar dicho procedimiento.

e. Los funcionarios, empleados, consultores y practicantes que requieran conexión remota a la red interna de la DIDADPOL (desde fuera de las oficinas), deberán tener previa aprobación de la Máxima Autoridad o gerente de su área. La Unidad de Tecnologías de Información UTI configurara un canal seguro VPN para evitar cualquier riesgo sobre la seguridad de la información.

f. Sera obligatorio que los proveedores y terceras partes, previo a tener acceso a la red de Datos de la DIDADPOL, deben cumplir con el proceso de autorización establecido por la Unidad de Tecnologías de Información UTI.

5.2. Gestión de acceso de usuarios

a. La Unidad de Tecnologías de Información UTI debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la institución, que contemple la creación, modificación, o deshabilitar las cuentas de usuario.

b. La Unidad de Tecnologías de Información UTI debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, previo comunicado de la Unidad de Recursos Humanos cuando los funcionarios, empleados, consultores y practicantes finalizan relación laboral, toman licencias, vacaciones, son trasladados o cambian de puesto en la Institución.

c. La Unidad de Tecnologías de Información UTI debe asegurarse que los sistemas de información posean protocolos de doble autenticación en sus inicios de sesión.

d. Los funcionarios, empleados, consultores y practicantes de DIDADPOL deben poseer un usuario de inicio de sesión en sus computadoras, celulares, Tablet u otros dispositivos asignados por la institución.

5.3. Responsabilidad de acceso de los usuarios

a. Los funcionarios, empleados, consultores y practicantes de la plataforma tecnológica, los servicios de red y los sistemas de información de la DIDADPOL deben hacerse responsables de las acciones realizadas en los mismos, así como de los usuarios y contraseñas asignadas para el acceso a estos.

b. Los funcionarios, empleados, consultores y practicantes de la DIDADPOL no deben compartir las contraseñas con nadie, ni escribirlas en lugares visibles, estas deben ser tratadas como información sensible y confidencial. Cualquier situación de vulnerabilidad que pueda pasar será responsabilidad directa del funcionario, empleado, consultor o practicante.

c. Cualquier funcionario, empleado, consultor o practicante que sospeche que sus usuarios o contraseñas han sido comprometidas, debe informar del incidente a la Unidad de Tecnologías de Información UTI, la cual realizara el proceso pertinente.

5.4. Control de acceso a Sistemas y Aplicaciones

La Máxima Autoridad, gerentes de área y jefes de unidades como propietarios de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, alertarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

La Unidad de tecnologías de Información UTI, como responsable de la administración de dichos sistemas de información y aplicativos, gestionaran para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso. Así mismo, vigilará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso y evitar accesos no autorizados a los sistemas administrados.

a. La Dirección, los gerentes y jefes de unidades propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, atendiendo los procedimientos establecidos.

b. La Unidad de Tecnologías de Información UTI debe tener un procedimiento para asignación y monitorear periódicamente los perfiles definidos en los sistemas de información y aplicaciones en la DIDADPOL.

c. La Unidad de Tecnologías de Información UTI debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas, preproducción y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

d. La Unidad de Tecnologías de Información UTI debe asegurar que los sistemas de información en sus menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

e. La Unidad de Tecnologías de Información UTI debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

f. La Unidad de Tecnologías de Información UTI es responsable de renovar en plazos cortos, todas las contraseñas con las cuales administra el acceso y control de dispositivos, plataformas tecnológicas, servicios y cualquier otra forma de gestión de información dentro de la DIDADPOL.

g. La Unidad de Tecnologías de Información UTI es responsable de asegurarse que los usuarios o perfiles por defecto de los equipos tecnológicos sean inhabilitados o eliminados.

h. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y sitios web, excepto aquellas específicamente clasificadas como públicas.

i. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.

j. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

k. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben asegurar que no se despliegan en la pantalla, las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

l. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.

m. La Unidad de Tecnologías de Información UTI por medio los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico institucional previamente registradas en los aplicativos, los cuales deben tener un

periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.

n. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.

o. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben establecer que periódicamente se revalide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

p. La Unidad de Tecnologías de Información UTI debe restringir el acceso al código fuente de los programas a personal no autorizado.

q. Los funcionarios, empleados, consultores y practicantes de la DIDADPOL, son responsables de tomar las medidas adecuadas para seleccionar y asegurar que sus contraseñas sean robustas y confiables, evitando utilizar las mismas contraseñas para los diferentes accesos a sistemas de información, plataformas tecnológicas y correo electrónico.

r. Los funcionarios, empleados, consultores y practicantes de la DIDADPOL que deseen tener acceso algún equipo tecnológico de funcionarios, empleados, consultores o practicantes que esté ausente por incapacidad o vacaciones, debe enviar un correo electrónico solicitando dicho acceso a la Unidad de Tecnologías de Información UTI con previa autorización del gerente de área, jefe de unidad o Máxima Autoridad de la Institución.

6. CRIPTOGRAFÍA

Los funcionarios, empleados, consultores y practicantes que manejarán la información de la institución clasificada como confidencial, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

6.1. Políticas de uso de los controles criptográficos

a. La Unidad de Tecnologías de Información UTI debe almacenar y/o transmitir la información digital clasificada como confidencial bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

b. La Unidad de Tecnologías de Información UTI debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información confidencial, cuente con mecanismos de cifrado de datos.

c. La Unidad de Tecnologías de Información UTI debe asegurar que los equipos portátiles tecnológicos de la Institución, deban mantener un sistema de cifrado de disco duro, para evitar acceso a la información de la institución por personal no autorizado.

d. La Unidad de Tecnologías de Información UTI deben cifrar la información confidencial y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.

e. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben asegurarse de que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por esta política.

6.2. Gestión de Claves

a. La Unidad de Tecnologías de Información UTI debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.

b. La Unidad de Tecnologías de Información UTI debe desarrollar y establecer un procedimiento de duración de las claves de cifrado a lo largo de todo su ciclo de vida.

7. SEGURIDAD FÍSICA Y DEL ENTORNO

La DIDADPOL proveerá de oficinas y velará por la efectividad de los mecanismos de seguridad física y control de accesos, asegurando el perímetro de las instalaciones en todas sus oficinas a nivel nacional. Así mismo controlara amenazas físicas internas y externas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentra equipo tecnológico y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

7.1. Perímetro de Seguridad Física

a. La DIDADPOL debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implementados en las instalaciones a nivel nacional.

b. La Máxima Autoridad, gerente y jefes de unidad deben velar porque las contraseñas de sistemas de alarma, cajas fuertes, armas, llaves, tarjetas de acceso y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los funcionarios, empleados, consultores y practicantes autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos sean transferidos a otros empleados de la institución.

c. La Máxima Autoridad, gerentes y jefes de unidades que cuenten con áreas restringidas, deben autorizar cualquier ingreso temporal, evaluando la pertinencia del ingreso; así mismo, deben delegar personal para llevar el registro y supervisión de cada ingreso a sus áreas.

d. La Gerencia Administrativa Financiera debe identificar mejoras a los mecanismos de seguridad física actuales y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física en las instalaciones de la DIDADPOL.

e. La Gerencia Administrativa Financiera debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de la DIDADPOL a nivel nacional.

f. La Unidad de Tecnologías de Información UTI establecerá procesos para el ingreso de personal autorizado de la Institución y proveedores al Centro de Datos.

g. La Unidad de Tecnologías de Información UTI debe manejar registro digital o físico del ingreso del personal de la institución o proveedores autorizados que ingresen al Centro de Datos y a los Centros de Cableado que están bajo su custodia.

h. En los eventos de finalización laboral o cambio de puesto de un empleado de la Unidad de Tecnologías de información UTI autorizado al acceso del Centro de Datos y Centro de Cableado, se deberá restringir y desactivar de manera inmediata los privilegios de acceso físico que tenga asignados.

i. La Unidad de Tecnologías de Información UTI debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica y sistemas de información ubicados en el Centro de Datos; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

j. La Unidad de Tecnologías de Información UTI debe velar porque los recursos de la plataforma tecnológica de la DIDADPOL ubicados en el centro de datos se encuentran protegidos contra fallas o interrupciones eléctricas.

k. La Unidad de Tecnologías de Información UTI debe certificar que el Centro de Datos y los Centro de Cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

l. La Unidad de Tecnologías de Información UTI debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos sin afectar las labores diarias.

m. La Unidad de Logística y Bienes de la DIDADPOL deberán utilizar las áreas de carga y descarga destinadas en la Institución, cumpliendo con protocolos de acceso establecidos y registros de ingreso y salida del personal.

n. Los ingresos y egresos de los funcionarios, empleados, consultores, practicantes, proveedores, terceras partes y visitantes a las instalaciones de la DIDADPOL a nivel nacional deben ser registrados digital o físicamente cumpliendo con los controles físicos implementados.

o. Los funcionarios, empleados, consultores, practicantes y proveedores deben portar el carnet que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de DIDADPOL a nivel nacional; en caso de pérdida del carnet o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible a la Unidad de Recursos Humanos.

p. Los funcionarios, empleados, consultores, practicantes, proveedores y visitantes de la DIDADPOL no deben intentar ingresar a áreas a las cuales no tengan autorización.

q. Los ciudadano o miembros de la Secretaria de Seguridad y de la Carrera Policial no podrán poseer celular, dispositivo de grabación o cámara fotografica en tomas de declaraciones o audiencias de descargos, por temas de confidencialidad de la información.

7.2. Seguridad de los equipos

La DIDADPOL para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la institución que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

a. La Unidad de Tecnologías de Información UTI deben asegurar que los equipos tecnológicos estén protegidos contra fallos de alimentación y otras alteraciones que puedan causar daños a los equipos.

b. La Unidad de Tecnologías de Información UTI debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de DIDADPOL.

c. La Unidad de Tecnologías de Información UTI debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la institución.

d. La Unidad de Tecnologías de Información UTI debe establecer estándares de configuración segura para los equipos de cómputo asignados a los funcionarios, empleados, consultores y practicantes de la institución.

e. La Unidad de Tecnologías de Información UTI debe establecer las condiciones que deben cumplir los equipos de cómputo de personal, proveedores o terceras partes, que requieran conectarse a la red de datos (invitados) de la institución, y

así poder verificar que se cumplan de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

f. La Unidad de Tecnologías de Información UTI debe aislar los equipos tecnológicos críticos de áreas sensibles para proteger su acceso de los demás los funcionarios, empleados, consultores y practicantes de la red de la Institución.

g. La Unidad de Tecnologías de Información UTI debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios, empleados, consultores y practicantes de la institución, ya sea cuando son dados de baja o cambian de persona.

h. La Unidad de Tecnologías de Información UTI es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos con previa autorización de la Unidad de Bienes; por consiguiente, está prohibido la disposición que pueda hacer cualquier funcionario, empleado, consultor y practicante de los recursos tecnológicos de la institución.

i. La Unidad de Tecnologías de Información UTI proporcionara las instrucciones técnicas que deben acoger los funcionarios, empleados, consultores y practicantes acerca de las computadoras, dispositivos móviles y demás recursos tecnológicos.

j. La Unidad de Tecnologías de Información UTI será la única responsable de la instalación, reparación o retiro de cualquier componente de hardware o software de los equipos tecnológicos de la institución. Los funcionarios, empleados, consultores y practicantes no podrán por ningún motivo llevar el equipo tecnológico a ser reparado por un proveedor externo.

k. Los equipos de tecnologías destinados a descargos deben ser reportados a la Unidad de Bienes para su respectivo proceso interno, la Unidad de Tecnologías

de la información UTI debe asegurarse hacer un proceso de borrado seguro de los mismos.

l. Los funcionarios, empleados, consultores y practicantes cuando se les presente una falla o problema de hardware o software en un equipo tecnológico propiedad de DIDADPOL deberá informar a la Unidad de Tecnologías de Información UTI, con el fin de recibir una asistencia adecuada. Por ningún motivo podrá intentar manipular el equipo. Exceptuando las oficinas regionales las cuales podrán hacerlo bajo estrictas supervisiones de un técnico de la Unidad de Tecnologías de Información UTI.

m. Los funcionarios, empleados, consultores y practicantes de la institución deben bloquear la sesión en su computadora en el momento de abandonar su puesto de trabajo.

n. Los funcionarios, empleados, consultores y practicantes de la DIDADPOL no deben dejar encendidas las computadoras u otros recursos tecnológicos en horas no laborables.

o. Los funcionarios, empleados, consultores y practicantes a los cuales se le haya asignado un equipo tecnológico para realizar actividades fuera de la institución, deberán darles el debido uso y cuidado.

p. Los funcionarios, empleados, consultores y practicantes deberán transportar los equipos tecnológicos con las medidas de seguridad apropiadas, que garanticen su integridad física.

q. Los funcionarios, empleados, consultores y practicantes en caso de pérdida o robo de un equipo tecnológico asignado por la DIDADPOL, estarán obligados a informar forma inmediata a la unidad de Bienes para que se inicie el trámite interno y presentar por escrito un informe del incidente ocurrido.

r. Los funcionarios, empleados, consultores y practicantes, deben asegurar que sus escritorios al terminar la jornada laboral, se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones y que estos sean almacenados bajo las protecciones de seguridad necesarias.

8. SEGURIDAD DE LAS OPERACIONES

a. La Unidad de Tecnologías de Información UTI debe mantener manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de la DIDADPOL.

b. La Unidad de Tecnologías de Información UTI debe efectuar la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la institución.

c. La Unidad de tecnologías de Información UTI debe proveer los recursos necesarios para la implementación de controles que permitan la separación de ambientes de desarrollo, pruebas, preproducción y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

d. La Unidad de Tecnologías de Información UTI capacitará a los oficiales de denuncias, investigadores y técnicos legales de las diferentes áreas en la extracción de Información de dispositivos de almacenamiento (celulares, USB, CD/DVD), en caso de sobrepasar los conocimientos dados en las capacitaciones o manuales podrán solicitar apoyo a la Unidad de Tecnologías de Información UTI para la extracción de información en toma de denuncias, toma de declaraciones, y audiencias.

e. Los funcionarios, empleados, consultores y practicantes tienen la obligación de mantenerse actualizados con la última documentación y los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la institución publicados por la Unidad de Tecnologías de Información UTI.

9. PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO (MALWARE)

La Unidad de Tecnologías de Información UTI proporcionara los mecanismos necesarios para garantizar la protección de la información y recursos tecnológicos que se manejan en la institución, adoptando controles que eviten la divulgación, modificación o daño permanente ocasionados por el contagio de software maliciosos. También creando mecanismos para generar una cultura de seguridad con todo el personal de la institución frente ataques de software maliciosos.

a. La Unidad de Tecnologías de Información UTI debe instalar herramientas como antivirus, antimalware, antispam y antispyware en los equipos tecnológicos, reduciendo el contagio de software malicioso y que respalden la seguridad de la información contenida y administrada en la plataforma de la DIDADPOL.

b. La Unidad de Tecnologías de Información UTI debe asegurarse mantener activa las licencias de antivirus, antimalware, antispam y antispyware, manteniendo activa las actualizaciones periódicas de las bases de datos de firmas del proveedor de servicios.

c. La Unidad de Tecnologías de Información UTI debe asegurarse que la información almacenada en la plataforma tecnológica de la DIDADPOL sea escaneada periódicamente, incluyendo la contenida y transmitida por el servicio del correo electrónico.

d. Los funcionarios, empleados, consultores y practicantes deben asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes

conocidas y seguras evitando el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

e. Los funcionarios, empleados, consultores y practicantes que sospechen o detecten alguna infección por software malicioso deben notificar a la Unidad de Tecnologías de Información UTI vía Sistema de Ticket, la cual tomara las medidas de control correspondientes.

10. COPIAS DE RESPALDOS DE LA INFORMACIÓN

La DIDADPOL debe proporcionar las herramientas y recursos para la realización de copias de respaldo de la Información. La Unidad de Tecnologías de Información UTI debe asegurarse de realizar copias de seguridad de información definiendo estrategias para periodos de respaldos y almacenamiento de información.

La DIDADPOL debe velar que la información crítica sea almacenada en una ubicación diferente a las instalaciones donde se encuentra dispuesta. Dicho sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

a. La Unidad de Tecnologías de Información UTI debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos, para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada, aplicando los accesos dependiendo puesto y funciones.

b. La Unidad de Tecnologías de Información UTI debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para comprobar su integridad y posibilidad de uso en caso de ser necesario.

c. La Unidad de Tecnologías de Información UTI debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

d. La Unidad de Tecnologías de Información UTI debe instalar software que realice respaldos de forma automática en tiempo real en las computadoras activas propiedad de la DIDADPOL.

e. La Unidad de Tecnologías de Información UTI, a través de los funcionarios, empleados, consultores y practicantes, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

f. Los funcionarios, empleados, consultores y practicantes de la DIDADPOL tienen responsabilidad de identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

11. REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

La Unidad de Tecnología de Información UTI debe realizar un monitoreo permanente del uso que le dan los funcionarios, empleados, consultores, practicantes a los recursos de las plataformas tecnológicas y los sistemas de información de la Institución de la DIDADPOL. Además, velará por la custodia de los registros de auditoría cumpliendo con los periodos de retención establecidos para dichos registros.

a) La Unidad de Tecnologías de Información UTI debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información de la DIDADPOL.

b) La Unidad de Tecnologías de Información UTI debe certificar la integridad y disponibilidad de los registros de auditoría generados en la plataforma tecnológica y los sistemas de información de la DIDADPOL, estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

c) La Unidad de Tecnologías de Información UTI a través de los desarrolladores deben generar registros (logs) de auditoría de las actividades realizadas por los funcionarios, empleados, consultores, practicantes y administradores de los sistemas de información desarrollados. Se deben utilizar controles de integridad sobre dichos registros.

d) La Unidad de Tecnologías de Información UTI a través de los desarrolladores deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas.

e) La Unidad de Tecnologías de Información UTI debe configurar los relojes de todos los sistemas de tratamiento de la información dentro de Institución, permitiendo estar sincronizados con una única fuente de tiempo precisa y acordada.

12. CONTROL AL SOFTWARE OPERATIVO

LA DIDADPOL a través de la Unidad de Tecnologías de Información UTI, designará responsables y establecerá procedimientos para controlar la instalación de software operativos, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

a. La Unidad de Tecnologías de Información UTI será la única autorizada para la instalación de software operativos en los equipos tecnológicos.

b. La Unidad de Tecnologías de Información UTI solamente instalara el software oficial, original y/o libre que vayan acorde a las labores de los funcionarios, empleados, consultores y practicantes dependiendo su perfil de puesto.

c. La Unidad de Tecnologías de Información UTI debe asegurarse que el software operativo instalado en los equipos tecnológicos de la DIDADPOL cuenta con soporte de los proveedores.

d. La Unidad de Tecnologías de Información UTI debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Realizando pruebas anticipadas que permitan asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

13. GESTIÓN DE VULNERABILIDADES

La Unidad de Tecnologías de Información UTI, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica y sistemas de información por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar las correcciones sobre los hallazgos arrojados por dichas pruebas.

a. La Unidad de Tecnologías de Información UTI debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas y hacking ético.

b. La Unidad de Tecnologías de Información UTI debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas tanto en la plataforma tecnológica y los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.

c. La Unidad de Tecnologías de Información UTI debe generar, ejecutar y monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica de la DIDADPOL.

14. SEGURIDAD DE LAS COMUNICACIONES

La Unidad de Tecnologías de Información UTI usara los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, velara por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información confidencial de la institución.

14.1. Gestión y aseguramiento de las redes de datos

a. La Unidad de Tecnologías de Información UTI debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la DIDADPOL.

b. La Unidad de Tecnologías de Información UTI debe implementar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos de la institución.

c. La Unidad de Tecnologías de Información UTI debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la institución.

d. La Unidad de Tecnologías de Información UTI debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

e. La Unidad de Tecnologías de Información UTI debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la institución en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

f. La Unidad de Tecnologías de Información UTI debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la DIDADPOL.

14.2. Correo Electrónico Institucional

La importancia del correo electrónico institucional como herramienta para proveer la comunicación entre los funcionarios, empleados, consultores, practicantes y proveedores, proporcionará un servicio idóneo y seguro para la ejecución de las actividades, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

a. La Unidad de Tecnología de Información UTI debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico institucional.

b. La Unidad de Tecnologías de Información UTI debe garantizar un protocolo de seguridad en el envío y recepción de mensajes de correos electrónicos, para proteger su contenido y garantizar su disponibilidad e integridad. Evitando que correos electrónicos institucional sea interceptados por personal no autorizados.

c. La Unidad de Tecnologías de Información UTI debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico institucional.

d. La Unidad de Tecnologías de Información UTI debe establecer procedimientos e implementar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

e. La Unidad de Tecnologías de Información UTI debe generar campañas para concientizar tanto a los funcionarios, empleados, consultores y practicantes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

f. La Unidad de Tecnologías de Información UTI debe garantizar un protocolo adicional de seguridad en el envío y recepción de mensajes de correo electrónico institucional, de manera de proteger su contenido y garantizar su disponibilidad e integridad. Evitando que correos electrónicos entre los funcionarios, empleados, consultores y practicantes puedan ser interceptados por personal no autorizado.

g. La Unidad de Tecnologías de Información UTI asignara un correo electrónico institucional individual a los funcionarios, empleados, consultores y practicantes, por consiguiente, bajo ninguna circunstancia se debe utilizar el correo electrónico institucional que no sea el suyo.

h. La Unidad de Tecnologías de Información UTI no está en la obligación por ningún motivo de darle un respaldo de su correo electrónico institucional a un funcionario, empleado, consultor y practicante en caso de terminación laboral.

i. Los funcionarios, empleados, consultores y practicantes de la DIDADPOL deben ser conscientes que en caso que amerite ser auditado su correo electrónico institucional, la Unidad de Tecnologías de Información UTI tiene la potestad, siempre y cuando haya justificación y autorización por escrito parte del gerente de área o Máxima Autoridad de la Institución.

j. Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada funcionario, empleado, consultor y practicante apegados a la Misión de DIDADPOL. Por ende, el correo institucional no debe ser utilizado para actividades personales, como inscripciones de plataformas bancarias, educativas, streaming, o demás fines

personales; Así mismo no debe ser utilizado para la creación o la distribución de mensajes ofensivos, acerca de raza, género, discapacidad, orientación sexual, pornografía, creencias religiosas, creencias políticas o étnicas.

k. Todos los mensajes enviados deben respetar el estándar de formato e imagen institucional definidos por la DIDADPOL y deben conservar en todos los casos el mensaje legal institucional de confidencialidad, aplicándose dicho literal a las cuentas de correos electrónicos institucionales de los funcionarios, empleados, consultores y practicantes de la DIDADPOL.

l. Todo funcionario, empleado, consultor o practicante que tenga una cuenta de correo institucional asignada, será el encargado del misma y responsable de todas las acciones que se lleven a cabo en su utilización.

m. Los funcionarios, empleados, consultores y practicantes no deben abrir ningún correo electrónico de remitentes desconocidos, en caso de recibir un correo electrónico de esta naturaleza, abrirlo por accidente o de forma deliberada, debe informarse inmediatamente al personal de la Unidad Tecnologías de Información UTI para tomar las medidas preventivas o correctivas pertinentes.

n. Los funcionarios, empleados, consultores y practicantes no deberán utilizar el correo personal en la red interna de DIDADPOL, evitando fuga de información de la misma.

o. Los funcionarios, empleados, consultores y practicantes no deberán utilizar el correo personal para fines laborares. En caso de necesitar tener acceso al correo electrónico institucional fuera de las oficinas de la DIDAPDOL podrán hacerlo vía navegador web.

14.3. Uso Adecuado De Internet

La DIDADPOL consciente de la importancia del Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los funcionarios, empleados, consultores y practicantes que así lo requieran para el desarrollo de sus actividades diarias en la institución.

La Unidad de Tecnologías de Información UTI debe definir normas para controlar y limitar el uso del internet desde cualquier dispositivo conectado a la red de la DIDADPOL. Asegurando que los funcionarios, empleados, consultores, practicantes, proveedores y terceras partes utilicen el Internet de manera segura y responsable.

a. La Unidad de Tecnologías de Información UTI debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

b. La Unidad de Tecnologías de Información UTI de Información debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

c. La Unidad de Tecnologías de Información UTI debe monitorear continuamente el canal o canales del servicio de Internet y llevar registros de los mismos.

d. La Unidad de Tecnologías de Información UTI debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios catalogados como restringidos.

e. La Unidad de Tecnologías de Información UTI debe generar registros de la navegación y los accesos de los funcionarios, empleados, consultores, practicantes, proveedores y terceras partes a Internet, así como establecer e

implementar procedimientos de monitoreo sobre la utilización del servicio de Internet.

f. Los funcionarios, empleados, consultores y practicantes que usan el servicio de Internet de la DIDADPOL deben hacer uso del mismo en relación con las actividades laborales que así lo requieran su puesto.

g. Los funcionarios, empleados, consultores, practicantes, proveedores, terceras partes no deberán acceder a páginas relacionadas con pornografía, drogas, alcohol, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas por la DIDADPOL.

h. Los funcionarios, empleados, consultores y practicantes no tienen permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros de la DIDADPOL.

14.4. Intercambio de Información

La DIDADPOL, asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con terceras partes con quienes se realice dicho intercambio. La institución velará por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

a. La Máxima Autoridad debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre la institución y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el

incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por la DIDADPOL a las terceras partes con quienes se establecen estos acuerdos.

b. La Máxima Autoridad de DIDADPOL y la Gerencia Administrativa debe asegurar en los contratos que se establezcan con proveedores o terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales por la divulgación no autorizada de información de la institución que les ha sido entregada en razón por cumplir con los objetivos estratégicos de la DIDADPOL.

c. La Unidad de Tecnologías de Información UTI debe entregar servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan poder cumplir el procedimiento para el intercambio de información, con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

d. Los funcionarios, empleados, consultores y practicantes propietarios de los activos de información deben velar porque la información de la DIDADPOL sea protegida de divulgación no autorizada por parte de las terceras partes a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

e. Los funcionarios, empleados, consultores y practicantes propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceras partes deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

f. Los funcionarios, empleados, consultores y practicantes propietarios de los activos de información deben asegurarse de que el Intercambio de información (digital) solamente se realice si se encuentra autorizada, para poder cumplir con estas Políticas de Seguridad de la Información Institucional, así como del procedimiento de intercambio de información.

15. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

La DIDADPOL asegurará que el software adquirido y desarrollado tanto al interior de la institución, como por proveedores o terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos. La Unidad de Tecnologías de Información UTI incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido interna y/o externa.

15.1. Requisitos de seguridad en los sistemas de información

a. La Unidad de Tecnologías de Información UTI debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

b. La Unidad de Tecnologías de Información UTI debe establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

c. La Unidad de Tecnologías de Información UTI debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

d. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se requiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

e. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas o de código abierto, reconocidas en el mercado.

f. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.

g. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

h. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.

i. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben utilizar los protocolos de seguridad estandarizados en los aplicativos.

15.2. Desarrollo y sus Procesos de Soporte.

La DIDADPOL velará porque el desarrollo interno o externo de los sistemas de información cumplan con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se

asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la institución.

a. La Unidad de Tecnologías de información UTI es responsable de realizar las pruebas de los sistemas de información para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción, utilizando metodologías establecidas para este fin, documentando las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

b. La Unidad de Tecnologías de información UTI es responsable de aprobar las migraciones en los sistemas de información, entre los ambientes de desarrollo, pruebas, preproducción y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

c. La Unidad de Tecnologías de Información UTI debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas, preproducción y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

d. La Unidad de Tecnologías de Información UTI debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la DIDADPOL.

e. La Unidad de Tecnologías de Información UTI debe asegurase que los sistemas de información adquiridos o desarrollados por terceras partes cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

f. La Unidad de Tecnologías de Información UTI se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de

cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

g. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

h. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de la DIDADPOL; dicho soporte debe contemplar tiempos de respuesta aceptables.

i. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los ciudadanos, funcionarios, empleados, consultores y practicantes antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

j. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.

k. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos

desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.

l. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.

m. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

n. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.

o. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.

p. La Unidad de Tecnologías de Información UTI por medio de los desarrolladores deben implementar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, modificar y eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

q. La Unidad de Tecnología de Información UTI por medio de los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.

r. La Unidad de Tecnologías de Información UTI debe verificar que las pruebas de seguridad sobre los sistemas de información se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.

15.3. Datos de Prueba

La Unidad de Tecnologías de Información UTI de la DIDADPOL protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de preproducción y producción.

a. La Unidad de Tecnologías de Información UTI debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de preproducción y producción.

b. La Unidad de Tecnologías de Información UTI debe eliminar la información de los ambientes de pruebas y preproducción, una vez estas han concluido.

16. RELACION CON PROVEEDORES Y TERCERAS PARTES

La DIDADPOL establecerá mecanismos de control en sus relaciones con proveedores y terceras partes con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

Los funcionarios y empleados responsables de la realización y/o firma de contratos o convenios con proveedores y terceras partes, se asegurarán de la divulgación de las políticas, normas y procedimientos de seguridad de la información a dichas partes.

a. La DIDADPOL se asegurará por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores y terceras partes, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

b. La Máxima Autoridad, gerentes de áreas, jefes de unidades que supervisan contratos con proveedores o terceras partes deben divulgarle las políticas, normas y procedimientos de seguridad de la información de la DIDADPOL, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los proveedores o terceras partes se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

c. La Gerencia Administrativa Financiera será la responsable de llevar control y revisión de la provisión de servicios del proveedor. LA DIDADPOL deben controlar, revisar y auditar regularmente la provisión de servicios del proveedor.

d. La Unidad de Tecnologías de Información UTI, la Gerencia de Servicios Legales debe generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes y proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

e. La Unidad de Tecnologías de Información UTI y la Gerencia de Legal deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes y proveedores. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la terceras partes o proveedores contratados.

f. La Unidad de Tecnologías de Información UTI debe establecer las condiciones de conexión apropiada para los equipos de cómputo y dispositivos móviles de los terceras partes y proveedores en la red de datos de la DIDADPOL.

g. La Unidad de Tecnologías de Información UTI debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceras partes o proveedores de servicios.

h. La Unidad de Tecnologías de Información UTI debe mitigar los riesgos relacionados con proveedores o terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de la DIDADPOL.

17. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS

17.1. Reporte y Tratamiento de Incidentes de Seguridad

La DIDADPOL promoverá entre los funcionarios y empleados, el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información y los medios físicos de almacenamiento.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La Máxima Autoridad y a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

a. La Unidad de Tecnologías de Información UTI debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

b. La Unidad de Tecnologías de Información UTI debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar a la Máxima Autoridad en los que se considere pertinente.

c. Es responsabilidad de los funcionarios, empleados, consultores y practicantes de la DIDADPOL reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

d. En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, confidencial; los funcionarios, empleados, consultores y practicantes deben notificarlo a la Unidad de Tecnologías de Información UTI para que se registre y se le dé el trámite correspondiente en la oficina de responsabilidad y disciplina.

e. Los funcionarios, empleados, consultores y practicantes propietarios de los activos de información deben informar a la Unidad de Tecnologías de Información UTI, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

18. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DE LA INSTITUCIÓN

La DIDADPOL proporcionará los recursos suficientes para dar una respuesta efectiva a los funcionarios, empleados, consultores y practicantes en caso de contingencia o eventos catastróficos que se presenten en la institución y que afecten la continuidad de su operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos.

La DIDADPOL mantendrá canales de comunicación adecuados hacia los funcionarios, empleados, consultores, practicantes, proveedores y terceras partes interesadas.

18.1. Continuidad de la seguridad de la información

a. La Máxima Autoridad, gerentes de área y jefes de Unidades deben identificar al interior de sus áreas, procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

b. La Unidad de Tecnologías de Información UTI debe elaborar un plan de recuperación ante desastres para la plataforma tecnológica, sistemas de información, equipos tecnológicos y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.

c. La Unidad de Tecnologías de Información UTI debe participar activamente en las pruebas de recuperación ante desastres y notificar los resultados a la Máxima Autoridad.

18.2. Redundancia

a. La DIDADPOL proporcionara recursos para la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la institución.

b. La Unidad de Tecnologías de Información UTI debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos de la institución y la plataforma tecnológica que los apoya.

c. La Unidad de Tecnologías de Información UTI debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de la DIDADPOL.

d. La Unidad de Tecnologías de Información UTI, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el poder cumplir con los requerimientos de disponibilidad de la institución.

19. CUMPLIMIENTO

La DIDADPOL velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propondrá que el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

19.1. Cumplimiento de los requisitos legales y contractuales

a. La Gerencia de Servicio Legales y la Unidad de Tecnologías de Información UTI de la Información deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la institución y relacionados con seguridad de la información.

b. La Unidad de Tecnologías de Información UTI debe certificar que todo software que se ejecuta en la institución esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

c. La Unidad de Tecnologías de Información UTI debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en los equipos tecnológicos de la institución para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas corresponda únicamente al permitido.

19.2. Revisiones de la seguridad de la información

a. La Máxima Autoridad, gerencias de áreas y jefes de unidades deben asegurarse 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.

b. El enfoque de la institución para la gestión de la seguridad de la información y su implementación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información, debe someterse a una revisión independiente por la Unidad de Tecnologías de Información UTI a intervalos planificados o siempre que se produzcan cambios.

c. La Unidad de Tecnologías de Información UTI debe comprobar periódicamente que los sistemas de información cumplen las políticas y normas de seguridad de la información de la Institución.

19.3. Privacidad y Protección de Datos Personales

La DIDADPOL por medio de sus gerentes y jefes de unidades velaran por la protección de los datos personales de los investigados, testigos, denunciantes, de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para el manejo de datos personales en la DIDADPOL, obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la institución, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la DIDADPOL exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, empleados, consultores y practicantes, estableciendo los controles necesarios para preservar aquella información que la institución conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la institución y no sea publicada, revelada o entregada a personal no autorizado.

a. La DIDADPOL a través de la dirección, gerencias y unidades que procesan datos personales de los investigados, testigos y denunciantes, deben obtener la

autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la Institución.

b. Los funcionarios, empleados, consultores y practicantes deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información del personal de la institución, investigados, testigos, abogados etc. de cual tengan conocimiento en el ejercicio de sus funciones.

c. Es deber de los funcionarios, empleados, consultores y practicantes, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por correo electrónico, entre otros.

d. Los funcionarios, empleados, consultores y practicantes de la DIDADPOL deben aceptar el suministro de datos personales que pueda hacer la institución a las terceras partes, como ser entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoría interna o externa.