PROCURADURÍA PARA LA DEFENSA DE LOS DERECHOS HUMANOS

PDDH

V.B.

PROCURADURIA PARA LA DEFENSA DE LOS DERECHOS HUMANOS
DESPACHO
REPÚBLICA DE EL SALVADOR

"POLITICAS DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA PDDH"

Mayo de 2023

POLÍTICAS DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA PDDH

TABLA DE CONTENIDO

POLÍTICAS DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA PDDH

TABLA DE CONTENIDO

POLÍTICAS DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DE LA PDDH

INTRODUCCIÓN

La información y los recursos informáticos son activos importantes y vitales de la PDDH, por lo que, las máximas autoridades y todos los empleados en cualquier nivel jerárquico, tienen el deber de custodiarlos, preservarlos, utilizarlos y mejorarlos. Esto implica que se deben tomar las acciones pertinentes para asegurar que la información y los sistemas de información estén apropiadamente protegidos contra diversas clases de amenazas y riesgos, por lo que es imprescindible adoptarse y aplicarse medidas de seguridad, sin importar los medios en los cuales la información se genera y/o guarde: (en papel o en medios electrónicos); como se procesa (computadoras personales, servidores, correo electrónico o de voz, etc.) y cómo se transmite (en físico, correo electrónico, conversación telefónica, chat institucional, etc.).

Una política de seguridad efectiva se concibe como parte integral de un modelo de "Cultura de Seguridad y Control de la Información", para que los usuarios tomen conciencia de la necesidad imperativa de proteger la Información, los equipos, los programas de aplicación y los sistemas de información, así como las redes de datos. En donde, las reglas y los procedimientos son guiados por el acercamiento de los usuarios a la información y el trabajo.

Cualquier imprudencia, violación o incumplimiento en materia de seguridad puede ocasionar a la institución perjuicios de diversa índole y consideración. Es por ello que, los Usuarios deben estar conscientes que la seguridad es asunto de todos y, por tanto, debe conocer y respetar las políticas que la institución adopte en esta materia.

Las políticas de seguridad de las tecnologías de la Información y comunicación identifican las reglas y procedimientos para cada usuario que accede o usa los recursos tecnológicos de una institución, sean equipos informáticos o equipos periféricos que constituyen herramientas de trabajo para la gestión de resultados.

MARCO LEGAL

El marco legal de la PDDH se origina en la Constitución de la República y en su ley de creación, cuyos textos principales, se presenta a continuación.

Constitución de El Salvador

Art. 194. Corresponde al Procurador para la defensa de los derechos humanos:

1. Velar por el respeto y la garantía a los derechos humanos;
2. investigar, de oficio o por denuncia que hubiere recibido, casos de violaciones a los derechos humanos;
3. Asistir a las presuntas víctimas de violaciones a los derechos humanos;
4. Promover recursos judiciales o administrativos para la protección de los derechos humanos;
5. Vigilar la situación de las personas privadas de su libertad. Será notificado de todo arresto y cuidará que sean respetados los límites legales de la detención administrativa;
6. Practicar inspecciones, donde lo estime necesario, en orden a asegurar el respeto a los derechos humanos;
7. Supervisar la actuación de la administración pública frente a las personas;
8. Promover reformas ante los órganos del estado para el progreso de los derechos humanos;
9. Emitir opiniones sobre proyectos de leyes que afecten el ejercicio de los derechos humanos;
10. Promover y proponer las medidas que estime necesarias en orden a prevenir violaciones a los derechos humanos;
11. Formular conclusiones y recomendaciones pública o privadamente;
12. Elaborar y publicar informes;
13. Desarrollar un programa permanente de actividades de promoción sobre el conocimiento y respeto de los derechos humanos;
14. Las demás que le atribuyen la constitución o la ley

Ley de la Procuraduría para la Defensa de los Derechos Humanos[1]

El Art. 11, Las atribuciones del Procurador de los Derechos Humanos, establecidas en el artículo 194 de la Constitución de la República de El Salvador.

Art. 12: Además de las atribuciones contempladas en el artículo anterior, el Procurador tendrá las siguientes:

1. Velar por el estricto cumplimiento de los procedimientos y plazos legales en los distintos recursos que hubiere promovido o en las acciones judiciales en que se interesare;
2. Velar por el respeto a las garantías del debido proceso y evitar la incomunicación de los detenidos;
3. Llevar un registro centralizado de personas privadas de su libertad y de centros autorizados de detención;
4. Presentar propuestas de anteproyectos de leyes para el avance de los derechos humanos en el país;
5. Promover la firma, ratificación o adhesión a tratados internacionales sobre derechos humanos;
6. Emitir resoluciones de censura pública contra los responsables materiales o intelectuales de violaciones a los derechos humanos;
7. Procurar la conciliación entre las personas cuyos derechos han sido vulnerados y las autoridades o funcionarios señalados como presuntos responsables, cuando la naturaleza del caso lo permita;
8. Crear, fomentar y desarrollar nexos de comunicación y cooperación con organismos de promoción y defensa de los derechos humanos, gubernamentales, intergubernamentales y no gubernamentales, tanto nacionales como internacionales y con los diversos sectores de la vida nacional;
9. Emitir el reglamento para la aplicación de la presente ley y los reglamentos internos que fueren necesarios;
10. Nombrar, remover, conceder licencias y aceptar renuncias a los funcionarios y empleados de la institución;
11. Elaborar el proyecto de presupuesto anual y remitirlo a la instancia correspondiente;
12. Las demás que le atribuyan la Constitución o la Ley.

[1] Decreto Legislativo No. 183 del 20 de febrero de 1992, publicada en Diario Oficial No. 45, Tomo 314 del 3 de marzo del mismo año.

Ley de Transparencia y Acceso a la Información Pública[2]

En particular lo establecido en el Art. 3 (fines de la Ley) incisos "e. Modernizar la organización de la información pública, g. Promover el uso de las tecnologías de la información y comunicación y la implementación del gobierno electrónico y h. Proteger los datos personales en posesión de los entes obligados y garantizar su exactitud", así como las Formas de Divulgación de la Información, establecida en el Art. 18. "La información oficiosa a que se refiere este capítulo deberá estar a disposición del público a través de cualquier medio, tales como páginas electrónicas, folletos, periódicos u otras publicaciones, o secciones especiales de sus bibliotecas o archivos institucionales. El instituto fomentará que los entes obligados utilicen tecnologías de la información y que dentro de un plazo razonable la información esté a disposición del público. No obstante, ninguna institución podrá negar información so pretexto de no contar con la tecnología adecuada.

Plan Estratégico Institucional 2021-2023

Al respecto, la Procuraduría para la Defensa de los Derechos Humanos, ha establecido en su Plan Estratégico Institucional 2021-2023, tres Ejes Estratégicos:

a) Eje Estratégico 1: Protección de derechos humanos
b) Eje Estratégico 2: Promoción de derechos humanos
c) Eje Estratégico 3: Fortalecimiento y desarrollo institucional

El Eje Estratégico 3, tiene como objetivo "Impulsar cambios en la cultura organizacional enfocándose en el desarrollo de las capacidades técnicas, gerenciales y competencias del personal para que garanticen servicios de calidad a la población en un ambiente laboral respetuoso de los derechos humanos con un uso eficiente de los recursos"[3].

El fortalecimiento y desarrollo institucional, entre otros, considera a las Tecnologías de Información y Comunicación como elementos indispensables para potenciar el trabajo institucional, así como las capacidades técnicas de respuesta ante las violaciones de los derechos humanos, por parte de los funcionarios públicos, en este contexto, se vuelve necesaria la creación de la Política de Seguridad de las Tecnologías de Información y Comunicaciones, para el manejo y resguardo de la información de los procesos de denuncias y

[2] Decreto Legislativo No. 534, LEY DE ACCESO A LA INFORMACIÓN PÚBLICA,. DADO EN EL SALON AZUL DEL PALACIO LEGISLATIVO; San Salvador, a los dos días del mes de diciembre del año dos mil diez

[3] Procuraduría para la Defensa de los Derechos Humanos, Plan Estratégico Institucional (PEI) 2021-2023 - Pensamiento Estratégico, Pag.21

PARÁMETROS.

Al momento de crear las políticas de seguridad TI, es importante que se considere lo siguiente:

- Efectuar un análisis de riesgos informáticos para adecuar la política a la situación actual de la institución
- Es necesario reunirse con los responsables de los recursos o sistemas ya que son la principal fuente para establecer el alcance y definir las violaciones.
- Comunicar a todo el personal involucrado sobre el desarrollo de la política, informando los beneficios, riesgos y los elementos de seguridad
- Es necesario identificar quien tiene la autoridad de tomar las decisiones en cada departamento y unidad ya que, deben ser los más interesados en proteger los activos críticos de sus áreas.
- Monitorear los procedimientos y operaciones de la institución, para que podamos ir actualizando la política.

Para que la implementación de la política de seguridad sea exitosas y aceptadas por todos es necesario es que procedamos a realizar una especie de estrategia de difusión para hacerles ver al personal las razones por la que se quieren implementar la política, los beneficios que podemos obtener y sobre todo involucrar a todo el personal.

La presente Política de Seguridad**,** es aplicable a la administración de:

LA INFORMACIÓN: Datos ordenados, clasificados y almacenados en cualquier medio (magnético, papel, correo electrónico, conversación telefónica, chat, USB, etc.).

EL SOFTWARE: Conjunto de Sistemas Operacionales, programas, productos y aplicaciones que utiliza la PDDH**.**

EL HARDWARE: Conjunto de equipos informáticos, telecomunicaciones y redes que utiliza la PDDH

DEFINICIONES

Para los efectos de la aplicación de las presentes disposiciones y bajo la perspectiva de las tecnologías de información, deberán considerarse las siguientes definiciones:

Archivos: Conjunto de datos o instrucciones que se almacenan en el Disco Duro y/o cualquier otro medio de almacenamiento con un nombre que los identifica. Ejemplo: PLANILLAS.xlsx, donde PLANILLAS es el nombre y .xlsx es la extensión del archivo.

Aplicaciones de Software: Es el conjunto de instrucciones mediante las cuales el Hardware puede realizar las tareas ordenadas por el usuario. Está integrado por los programas, sistemas operativos y utilidades.

Autorización: Proceso o procedimiento oficial de la PDDH por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos del sistema de información.

CPU: (Unidad Central de Proceso): Es una parte del Hardware o equipo de informático que realiza el procesamiento de datos.

Contraseña: Password o clave para obtener acceso a un programa o partes de un programa determinado, una terminal o computadora personal (portátil o de escritorio), un punto en la red (fijo o inalámbrico), etc.

Contraseña Robusta: Password o clave que cumplen con las condiciones específicas de acuerdo a la normativa internacional para la seguridad de la información.

Cuenta de Usuario: Es el identificador único que utiliza un Sistema de Información en la autenticación de los usuarios autorizados.

Correo Corporativo: Servicio en línea que provee un espacio para la recepción, envío y almacenamiento de mensajes de correo electrónico por medio de Internet a través del dominio institucional de la PDDH (@pddh.gob.sv)

Cuenta de Correo Institucional: Asignación única para un usuario del correo electrónico institucional.

Encriptado: Cifrado o codificación de la información sensible que puede ser recibida o enviada desde o para los sistemas de información de la PDDH.

Disco duro: Medio utilizado para el almacenamiento de información. Cuando se almacena información en un disco, ésta se conserva incluso después de apagar el computador y se encuentra guardada de forma permanente en el interior del Hardware.

Disponibilidad: Característica relacionada con la facilidad y oportunidad de acceso a la información cuando sea requerida por los procesos de la PDDH para realizar sus tareas, o actividades en el marco de sus responsabilidades institucionales, ahora y en el futuro.

CD-ROM, DVD, USB, DISCOS DUROS: Medios utilizados para el almacenamiento de información, que puede introducirse y retirarse del drive del Hardware o de los puertos de comunicación de la computadora.

Equipos de informáticos: Son los dispositivos eléctricos, electrónicos y mecánicos que se emplean para procesar o consultar, transmitir, almacenar datos. (Hardware)

Hacker: Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no ser maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo.

Popularmente se le conoce como piratas informáticos a aquellos hackers que realizan acciones malignas con sus conocimientos.

Hardware: Partes físicas de un sistema de procesamiento de datos, por ejemplo, la CPU, el monitor, el impresor, teclado, ratón, módems, teléfonos, enrutador, Switches, etc.

Incidente: Es todo evento que surge a raíz de una definición inadecuada del alcance de un producto, mala práctica en el sistema, operación o una violación a las Políticas de Seguridad de la Información y que conlleva a una falla en la operatividad normal dentro de la PDDH.

Información: conjunto de datos sobre un suceso o fenómeno en particular que al ser ordenados en un contexto sirven para disminuir la incertidumbre y aumentar el conocimiento sobre Políticas de Seguridad de Las Tecnologías de Información y Comunicaciones es un tema específico. Es todo, lo que puede ser expresado a través de un lenguaje de programación y es utilizada por la PDDH durante el desarrollo de sus actividades y operaciones rutinarias.

Información Sensible: Información que por su naturaleza debe mantenerse bajo estrictas medidas de seguridad que garanticen el acceso sólo al personal autorizado y para un propósito previamente definido.

Información Interna: Es aquella información de uso interno que utilizan los empleados de la PDDH con el propósito de realizar las operaciones normales de la institución. Son ejemplos de información interna: los registros o datos obtenidos o generados de los usuarios.

Información Pública: Todo archivo, registro, dato o comunicación contenida en cualquier medio, documento, registro impreso, óptico o electrónico u otro que no haya sido clasificado como reservado y que está disponible para la distribución pública por medio de los canales autorizados, en congruencia con las disposiciones que se establecen en los lineamientos de la Ley de Transparencia y Acceso a la Información Pública.

Integridad: Es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados, así como su validez de acuerdo con los requerimientos de la PDDH.

Log o Bitácora: Archivo que registra movimientos y actividades de un determinado programa, utilizado como mecanismo de control y estadística.

Monitor: (pantalla): Permite visualizar electrónicamente la salida de datos de un computador.

Parche de Seguridad: Conjunto de instrucciones de corrección para un software en especial, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento, en el Código original de este.

Periféricos: Corresponde a cualquier dispositivo o equipo, tales como: impresoras, unidad ininterrumpida de poder (UPS), unidades de cinta, estabilizadores y reguladores de voltaje, mouse (ratón óptico o manual) teclado, unidades de CD y de DVD, teléfonos, enrutadores, Switches, antenas de comunicación, controles de acceso, toquen, cámaras, grabadoras de

video, parlantes, monitor, escáner, equipos biométricos, etc.

Programas (software): Conjunto de instrucciones que permiten manejar una tarea en procesamiento electrónico de datos, por ejemplo: office, módulo financiero, módulo de planillas, registro de afiliación, correo institucional, chat institucional, etc.

Protector de pantalla: Imagen o diseño móvil que aparece en la pantalla cuando transcurre un determinado período de tiempo durante el que no se mueve el ratón (Mouse) o se presiona una tecla. Los protectores de pantalla evitan que la pantalla resulte dañada como consecuencia de la presentación de áreas oscuras y luminosas en la misma posición durante largo tiempo.

Recursos informáticos: Software, hardware y redes que posee y/o utiliza la PDDH.

Riesgo de la Información: Es una combinación de la posibilidad de que una amenaza contra un activo de información ocurra aprovechando una vulnerabilidad y/o falla en un control interno, y la severidad del impacto adverso resultante.

Sistema: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso, generados para cubrir una necesidad u objetivo.

Sistemas Operativos: Es un programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación ejecutándose en modo privilegiado respecto de los restantes.

Software ilegal: Es el Software que se adquiere y se instala sin el consentimiento de la persona o empresa que lo desarrolla (propietario). Es también llamado Software Pirata, en donde su fabricante no obtiene ninguna contraprestación económica por su uso y sus derechos de autoría intelectual son violados. También se considera ilegal todo el software que no ha sido autorizado por la autoridad competente para ser utilizado en el equipo y/o las instalaciones de la PDDH aun cuando el usuario haya comprado una licencia de uso del mismo.

Terceros: Personas que no son empleados de la PDDH o instituciones diferentes a la misma. Ejemplo: Participantes, beneficiarios, proveedores regulares o potenciales de bienes y servicios, empresas candidatas a prestar servicios a la Institución, entes reguladores, consultores, etc.

Vulnerabilidad: Debilidad de un sistema, que da posibilidad de realizar alguna acción que afecte negativamente a éste.

OBJETIVO DE LA POLÍTICA DE SEGURIDAD

Preservar la seguridad, confidencialidad, integridad, disponibilidad de los sistemas, la información y los recursos tecnológicos que utilizan los empleados de la Procuraduría para la Defensa de los Derechos Humanos, PDDH.

La confidencialidad implica la protección de los recursos, la integridad asegura que las modificaciones de los recursos están siendo administrados y utilizados por vías autorizadas y la disponibilidad es el estado donde los sistemas y la información están siempre disponibles.

Las políticas de seguridad TIC es un documento que se va adaptando continuamente con la evolución de la institución y de los requerimientos del avance tecnológico, es decir, deben seguir un proceso de actualización periódica de acuerdo a los cambios organizacionales, para mencionar algunos: aumento del personal, desarrollo de sistemas o servicios, cambios en la infraestructura de tecnología, entre otras.

OBJETIVOS ESPECIFICOS

1. Consolidación de la seguridad como tema estratégico y concientización global sobre la importancia de la seguridad de la información.
2. Planeamiento y manejo de la seguridad más efectivos.
3. Mayor seguridad en el ambiente informático, minimizar los riesgos inherentes a la seguridad de la información y generar una mejor y oportuna reacción a incidentes de seguridad.
4. Orden en el trabajo bajo un marco normativo que evita la duplicidad de tareas y facilita el intercambio de información.
5. Incremento de la cooperación entre las Unidades Organizacionales, por ser la seguridad el interés común.
6. Mayor facilidad para la toma de decisiones.
7. Mejora de la imagen institucional.
8. Mayor control de la información recibida y/o proporcionada a terceros y aumento de la confianza de los mismos.

RESPONSABLES

La presente Política de Seguridad de la Información es aplicables a todas las áreas, departamentos, unidades y delegaciones departamentales de la PDDH y son de cumplimiento obligatorio por parte de todos los funcionarios y empleados de la institución, en cualquier nivel jerárquico, sean temporales o permanentes, definidos como los usuarios y administradores de la información y equipos informáticos, así como por otros usuarios que utilicen de una u otra

forma los sistemas de información o las redes tecnológicas de la PDDH.

En ese contexto, existen distintos niveles de responsabilidad en el manejo y uso de la información:

ADMINISTRADOR DE SISTEMAS: Es el responsable técnicamente de la administración, disponibilidad, seguridad y operación de un determinado sistema de información, en función de su responsabilidad institucional.

CUSTODIOS: Se denomina así a las personas o áreas que proporcionan servicios, sin que necesariamente conozcan la información que custodian, solamente la procesan, gestionan su almacenamiento y la hacen accesible.

DUEÑO: Es generalmente el titular del área funcional de un sistema específico en particular, con la potestad para definir el alcance, la operatividad y las limitantes del mismo y de autorizar el acceso a la información.

USUARIO: Es aquella persona, empleada de la PDDH, que crea, lee, introduce, cambia o actualiza la información almacenada en los Sistemas Informáticos de acuerdo con los privilegios, roles y autorizaciones que le son asignados. Para adquirir un perfil de usuario es necesaria la justificación y autorización por escrito previa del Dueño de la información o de la autoridad competente.

El incumplimiento de las presentes Políticas de Seguridad dará lugar a la aplicación de las sanciones establecidas de conformidad a la Ley de Transparencia y Acceso a la Información Pública, establecidas como atribuciones del Instituto de Acceso a la Información Pública, el Reglamento Interno de Trabajo de la PDDH y demás disposiciones internas relacionadas, sin perjuicio de las acciones civiles o penales que, en su caso, puedan resultar aplicables

POLITICAS DE SEGURIDAD

DEL ADMINISTRADOR DE SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN.

Con el propósito de homogenizar y centralizar todo lo relativo a la seguridad de la información, la PDDH deberá contar con la plaza de Jefe de las Tecnologías de Información, quien asumirá la responsabilidad de Administrador de Seguridad de las Tecnologías de Información y Comunicación de la institución, quien será nombrado por el o la Titular de la PDDH y estará subordinado a la Secretaría General, mientras no se hayan realizado cambios en el Reglamento de Operaciones y Funciones de la Procuraduría para la Defensa de los Derechos Humanos, en cuyo caso, el Titular designará su posición en la estructura organizacional de la institución, comprendiendo entre sus responsabilidades las siguientes:

- Promover y gestionar la implementación de una cultura de seguridad de la información por parte de todos los empleados de la PDDH.
- Documentar y proponer ante la Secretaría General las políticas, normas y procedimientos de seguridad de la información para su aprobación y presentación ante el Titular, cuando corresponda y velar por su implementación y cumplimiento.
- Dirigir las investigaciones y auditorias sobre incidentes y problemas relacionados con la seguridad de la información, así como recomendar las medidas de control pertinentes.
- Promover e implementar la continuidad de las operaciones y recuperación de la información en casos de desastres
- Velar por la protección de la propiedad intelectual
- Proponer y gestionar la implementación de medidas de prevención del fraude electrónico

DE LOS USUARIOS.

Los Usuarios son responsables de cumplir con todas las políticas de la PDDH relativas a la Seguridad de la Información y las comunicaciones, y en particular de:

a) Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la Información, Hardware y Software de la PDDH.

b) No divulgar por cualquier medio, información confidencial de la PDDH a personas no autorizadas.

c) Responder por todas y cada una de las transacciones efectuadas en el software con su usuario y contraseña asignada.

d) Proteger meticulosamente su contraseña y evitar que sea vista por otros usuarios en forma inadvertida.

e) No compartir o revelar su contraseña a otras personas empleados o ajenos la PDDH.

f) Seleccionar una contraseña segura que no tenga relación obvia con el usuario, sus familiares, la institución de trabajo y otras relaciones parecidas.

g) Reportar inmediatamente a su jefe inmediato, al Administrador de Seguridad Informática cualquier evento que pueda comprometer la seguridad de la PDDH y sus recursos informáticos o de sistemas, como, por ejemplo: contagio de virus informáticos, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

h) Proponer medidas de Seguridad de la Información que hagan que la PDDH tenga una operación cada vez más segura.

DE LA SEGURIDAD DE INFORMACIÓN SENSIBLE

a) Es responsabilidad de los usuarios velar por la integridad, confidencialidad, y disponibilidad de la información que acceda o maneje directamente, especialmente si dicha información ha sido clasificada como sensible.

b) Los usuarios son responsables de utilizar la información a la que tengan acceso, exclusivamente para el desempeño de su actividad profesional y laboral en la PDDH, no podrán facilitarla más que a aquellos otros empleados que necesiten conocerla para la misma finalidad y se abstendrá de usarla en beneficio propio o de terceros.

c) La información relativa a los empleados, y en general a sus datos personales, debe ser tratada como información confidencial, así como, aquella información clasificada como reservada de acuerdo a los preceptos establecidos en la Ley de Acceso a la Información Pública.

d) La información relativa a los empleados, funcionarios y Procuradores/as Adjuntas, incluida, en su caso, la relativa a remuneraciones, evaluaciones y revisiones médicas debe ser tratada con especial cuidado como información confidencial sensible del recurso humano.

e) El buen uso de las tecnologías que la PDDH ha puesto a disposición de sus empleados y funcionarios debe permitir el resguardo eficiente y eficaz de la información pública

f) Es responsabilidad de los usuarios garantizar que toda documentación en formato impreso, electrónico, etc., que contenga información sensitiva de los participantes, una vez utilizada, o que no pueda ser entregada al propietario, sea archivada de manera segura.

g) Es responsabilidad de los encargados de la gestión de archivos físicos, velar por la integridad de la información almacenada físicamente y que refleja las transacciones e información del participante o de la institución afiliada.

h) Cuando se traslade documentación física que contenga información sensible, por parte de cualquier empleado de la PDDH, ya sea que ingrese o salga de las oficinas principales/departamentales o transite entre las áreas funcionales, debe portar los expedientes y demás documentos dentro de un fólder o bolsa cerrada que no permita ver el contenido de estos (impedir la visión de la información).

DEL USO DE LAS ESTACIONES DE TRABAJO

a) El Usuario es responsable de mantener el Hardware que le ha sido asignado debidamente identificado para efectos de control de inventario. El Área responsable (Departamento de Activo Fijo) deberá mantener los registros de inventario debidamente actualizados.

b) Se prohíbe utilizar la Información, Hardware y Software, para realizar actividades diferentes a las estrictamente laborales, sean estas en su desempeño profesional como en el ámbito educativo.

c) Se prohíbe mover el Hardware, reubicarlo o llevarlo fuera de la PDDH sin el Visto Bueno de la Jefatura que lo tiene asignado y la debida autorización escrita extendida por el departamento de Activo Fijo y el traslado debe estar motivado por los intereses y objetivos laborales propios de la PDDH.

d) Se prohíbe instalar y utilizar en el hardware asignado para sus actividades laborales, software no autorizado o software ilegal. En los equipos de la PDDH sólo podrá utilizarse software legal y oficial y su instalación será exclusiva del Departamento de Tecnologías de Información.

e) Está prohibido modificar la configuración de hardware y software establecida por el Departamento de Tecnologías de Información. Tampoco está permitido hacer copias del software para fines personales.

f) Se prohíbe instalar en el Hardware de la PDDH, software propiedad del usuario, a menos que haya sido comprobado en forma rigurosa y que esté aprobado y autorizado su uso por la Jefatura de mayor jerarquía del usuario solicitante y el Departamento de Tecnologías de Información.

g) El Usuario es responsable de salvar (guardar) periódicamente la información de su equipo cuando esté utilizando el hardware para evitar que un corte de energía u otra falla del equipo, le haga perder la información de manera permanente.

h) El Usuario debe realizar su debido respaldo (Backup) de la información que generar o utiliza en su equipo, en forma periódica.

i) El Usuario es responsable de utilizar el método de suspensión que provee el sistema operativo de su computador al cual se accede únicamente por medio de la contraseña que se le ha sido asignada, evitando así que otras personas ingresen a sus archivos o en su defecto de bloquear la maquina mientras se mueva de su sitio de trabajo. Asimismo, siempre que sea posible el hardware deberá estar instalado de tal forma que no permita que visitantes o personas extrañas a la PDDH puedan tener acceso a ningún tipo de información, ya sea en pantalla, impresora o cualquier otro dispositivo.

j) El Usuario es responsable de apagar el hardware que tenga asignado cuando tenga que abandonar su estación de trabajo por períodos de tiempo superiores a una (1) hora. Deberá además bloquear su estación de trabajo durante cualquier ausencia temporal de su puesto de trabajo.

k) Es responsabilidad del Departamento de Recursos Humanos notificar al Departamento de Tecnologías de Información tan pronto un empleado termine su relación laboral con la PDDH y trabaje en un Hardware propio, para que proceda a eliminar la información propiedad de la PDDH contenida en el equipo y realizar la desinstalación del software Institucional.

l) El Usuario es responsable de mantener organizada la información en el disco duro y conservar en el mismo únicamente los archivos que necesita para llevar a cabo sus labores. Los archivos de uso personal como música, fotografías, videos, juegos, etc. estarán bajo la responsabilidad del usuario los daños que causaren al equipo o información de la PDDH por no acatar esta disposición.

m) El área de Soporte Técnico del Departamento de Tecnologías de Información eliminará bajo la instrucción y responsabilidad del usuario, la información confidencial contenida en el hardware que el usuario tenga asignado, antes de que dicho Hardware sea reparado o enviado fuera de la PDDH, Si esto no es posible, el usuario debe asegurarse de que la

reparación sea efectuada por empresas responsables, con las cuales se haya firmado un acuerdo de confidencialidad.

n) Se prohíbe el uso del hardware y software de la PDDH a terceros o personas extrañas al mismo, salvo autorización escrita de la Secretaría General o en su defecto de la Jefatura de Tecnologías de Información.

o) Es responsabilidad de los usuarios identificar y reportar a su Jefe inmediato, hardware y software no autorizado, así como la pérdida o robo de los mismos.

p) No debe dejarse desatendido en ningún momento el hardware, sobre todo si se está imprimiendo o se va a imprimir Información confidencial o si la misma se está enviando oficialmente a través del correo electrónico corporativo o a través de otros medios de comunicación como el fax.

q) Es responsabilidad del Usuario evitar el deterioro del Hardware, para lo cual deberá cumplir las siguientes reglas básicas:

- No ingerir ni dejar alimentos y/o bebidas cerca y/o encima del Hardware.
- No colocar objetos pesados encima del Hardware.
- Mantener alejado del Hardware cualquier elemento electromagnético como imanes, radios, etc.
- No colocar el Hardware en lugares inestables y/o expuestos a ser golpeados involuntariamente o que estén en riesgo de caer y dañarse parcial o totalmente.
- No abrir el Hardware. De ser necesaria dicha labor será llevada a cabo por el Área de Soporte Técnico del Departamento de Tecnologías de Información.
- Es responsabilidad de los Usuarios conservar siempre limpio su lugar de trabajo, así como su Hardware.
- Conservar los cables en buen estado, ordenados y correctamente conectados. No debe existir ningún tipo de tensión, evitando siempre el doblado de los mismos.

DE LOS USUARIOS Y LAS CONTRASEÑAS

a) Es responsabilidad del Departamento de Tecnologías de Información, asignar un nombre único de usuario y es responsabilidad del usuario tener una contraseña robusta reservada

en cada sistema informático, los cuales deberán ser confidenciales e intransferibles para garantizar su óptima identificación.

b) Se prohíbe asignar códigos de identificación de usuario genérico o universal, tales como: PDDH1, PDDH2, etc. Su utilización está restringida a procesos automáticos que se realicen en los sistemas y que no puedan cambiarse por usuarios personalizados.

c) Se prohíbe asignar códigos de identificación de usuario a personas que no sean empleados de la PDDH, a menos que estén debidamente autorizados, por la Jefatura de mayor jerarquía del área que corresponda, en este caso la Jefatura de Tecnologías de Información deberá dar su visto bueno y determinará los medios de control requeridos para evaluar el riesgo y que estos códigos se definan por tiempo limitado.

d) Ningún usuario o programa debe utilizar las contraseñas de administrador de sistemas, salvo personal autorizado por de la Jefatura del Departamento de Tecnologías de Información.

e) El área de soporte técnico del Departamento de Tecnologías de Información desactivará los Códigos de Identificación de Usuario que no sean usados por un período comprendido entre uno y tres meses, siempre y cuando no exista causa justificable para no estar presente en la institución (enfermedad, maternidad, permiso de trabajo, entre otros).

f) Los Códigos de Usuario que cumplan un período de tres (3) meses en estado de inactivos, deben pasar al estado de Cancelado en el sistema, al menos que haya causa justificada establecida en el numeral anterior.

g) Es responsabilidad del Usuario no guardar su contraseña en una forma legible en archivos en disco; tampoco debe escribirla en papel, dejarla en sitios donde pueda ser encontrada o compartirla o revelarla a cualquier otra persona. El usuario que viole esta normativa será responsable directo por todos los daños y perjuicios que resulten de tal violación.

h) Es responsabilidad del Usuario cambiar inmediatamente su contraseña cuando tenga indicio o razón suficiente para creer que ha sido comprometida, o de acuerdo a la política de seguridad establecida en este documento, para lo cual deberá contar con el respaldo de la Jefatura de Tecnologías de Información (cada 30 días calendarios).

i) Es responsabilidad del Usuario no usar contraseñas que sean idénticas o sustancialmente similares a contraseñas previamente empleadas.

j) La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. Es responsabilidad del Usuario cambiar en esta primera sesión su contraseña inicial por otra

contraseña robusta, el mismo día que se le entregue por parte del Departamento de Tecnologías de Información.

k) Se limita a tres (3) el número consecutivo de intentos infructuosos para introducir la contraseña de Usuario; después del tercero y último intento la cuenta involucrada queda bloqueada y se deberá notificar al Departamento de Tecnologías de Información, así como de hacer la solicitud de cambio, justificando el extravió de la misma, documentando cual ha sido el problema para tal evento y firmado por su Jefe inmediato.

l) Es responsabilidad del Usuario evitar que su contraseña esté visible en pantalla en cualquiera de los procesos en que la utilice (conexión, utilización, etc.).

m) Todo aplicativo debe ser auditable, es decir, debe permitir dejar rastro de todas las transacciones críticas generadas: bitácora (log) de transacciones y registro de entradas y salidas de usuarios.

n) Se prohíbe tener múltiples sesiones de usuario en diferente Hardware. Por ejemplo, su usuario en computadoras del Departamento de Recursos Humanos y otra en el Departamento Administrativo.

o) Ningún usuario puede tener más de un código de identificación de usuario para el acceso a una misma aplicación.

p) Es responsabilidad de Recursos Humanos que tan pronto un empleado termine su relación laboral con la PDDH, se proceda a realizar la cancelación de sus códigos de identificación de usuario y Contraseña, notificando al Departamento de Tecnologías de Información de tal cambio por escrito para hacer las gestiones necesarias de seguridad y de resguardo de la información propiedad de la PDDH.

q) Es responsabilidad del Usuario crear siempre contraseñas robustas, para ello deberá cumplir las siguientes reglas:

- No utilizar solamente letras o números, sino una combinación de ambos.
- No utilizar palabras reconocibles como nombres propios, palabras del diccionario o
- términos de programas de televisión, novelas y artistas, entre otros.
- No utilizar palabras en idiomas extranjeros.
- No utilizar información personal.
- No invertir palabras reconocibles.

- No utilizar la misma contraseña para todas las máquinas.
- Mezclar letras mayúsculas y minúsculas.
- Seleccionar una contraseña que pueda recordar.

r) Es responsabilidad del encargado del área que administra la seguridad de los usuarios, realizar una revisión periódica de al menos cuatro veces al año, de los accesos asignados a los usuarios.

DE LA POLÍTICA ANTIVIRUS

Responsabilidades de los Usuarios:

a) Utilizar el Antivirus autorizado por el Departamento de Tecnologías de Información de la PDDH, el cual tendrá disponible automáticamente cada vez que se conecte al dominio de la red.

b) Mantener el Antivirus permanentemente activo para que vigile constantemente todas las operaciones realizadas en el Sistema. Está terminantemente prohibido al Usuario desactivar el Antivirus.

c) Dar aviso inmediato al Departamento de Tecnologías de Información y apagar el Hardware asignado inmediatamente que detecte la presencia de un virus electrónico que no es eliminado por el Antivirus utilizado de manera institucional. Por motivo de seguridad, los mensajes o archivos adjuntos que contengan virus serán inmediatamente eliminados sin posibilidad de recuperación.

d) Revisar con el Antivirus sus unidades de CD/DVD, memorias USB (flash) antes de usarlas.

Prohibiciones:

a) Está terminantemente prohibido al Usuario ejecutar los archivos anexos a su correo electrónico si no provienen de una fuente reconocida y segura.

b) Queda terminantemente prohibido al Usuario compartir el disco duro del Hardware que tenga asignado, si necesita compartir alguna carpeta debe obtener la autorización correspondiente y sólo hacerlo a los usuarios destino.

DEL USO DEL CORREO ELECTRÓNICO

a) Queda terminantemente prohibido a los usuarios el envío de mensajes masivos a través de correo electrónico; excepto en el caso de correos oficiales los que podrán ser enviado por usuarios debidamente autorizados por la Secretaría General, o en su defecto por la Jefatura de Tecnologías de Información,

b) Es responsabilidad del Usuario enmarcar todos los mensajes que envíe a través de correo electrónico dentro de las normas mínimas de respeto y protocolo electrónico, siempre deberá incluir el tema o referencia del correo que remite (Asunto) pero sin incluir contenidos hostiles que molesten a los receptores del mismo, tales como: comentarios sobre sexo, raza, religión o preferencias sexuales; asimismo, es responsabilidad del Usuario reportar a su Jefe Inmediato la recepción de este tipo de mensajes, quien a su vez deberá reportarla al Jefe o Jefa del Departamento de Tecnologías de Información y al Administrador de Seguridad de la Información.

c) Es responsabilidad del Usuario evitar que su cuenta de correo electrónico sea utilizada por terceros (otros usuarios, proveedores, sindicatos, familiares, etc.).

d) Es responsabilidad del Usuario evitar que la información confidencial sea transmitida por medio de su cuenta de correo electrónico, salvo autorización previa del Jefe de área en cuyo caso los archivos deben viajar en forma segura o cifrada.

e) Es responsabilidad del Usuario evitar el uso de una cuenta de correo electrónico que pertenezca a otro usuario, si hay necesidad de hacerlo en caso de ausencias o vacaciones se debe recurrir por medio de las TIC a mecanismos alternos como redirección de mensajes.

f) Se prohíbe el uso de la cuenta de correo electrónico, para:

- Utilizar el correo institucional para mensajes de carácter personal.
- Enviar mensajes desde la cuenta de correo electrónico de un usuario con firma de otro.
- Acceder sin autorización a otra cuenta de correo electrónico.
- Transmitir mensajes de correo con información sensible o confidencial a personas u organizaciones externas sin autorización.
- Participar en cadenas de mensajes que congestionen la red de datos y que destruyen los equipos de comunicación de redes y que saturan los servidores de mensajería.

g) Es responsabilidad de los usuarios de correo electrónico mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.

h) Es responsabilidad del Usuario eliminar periódicamente de sus dispositivos de almacenamiento los mensajes que ya no necesite. Con esto se reducen los riesgos de que otros usuarios puedan acceder a esa información; y, además, se libera espacio en disco.

i) Ningún empleado de la PDDH está autorizado para monitorear los mensajes de correo electrónico, excepto el área que previamente esté autorizada por la Secretaría General o en su defecto por la Jefatura del Departamento de Tecnologías de Información. El monitoreo es realizado para cumplir con políticas internas en casos de sospechas de actividad no autorizada, investigaciones y otras razones del Titular; en estos casos la PDDH no está obligada a solicitar autorización alguna al Usuario involucrado.

j) Todos los mensajes enviados por medio de correo electrónico son propiedad de la PDDH y ésta, se reserva el derecho de acceder y revelar los mensajes enviados por este medio para cualquier propósito.

k) Queda terminantemente prohibido el uso de servicios de mensajería instantánea (Chat) no institucional, utilizando el acceso de Internet de la PDDH, si para sus funciones necesita este servicio debe obtener la autorización correspondiente y utilizarlo sólo para asuntos laborales.

DEL USO DE INTERNET

a) Es responsabilidad del Usuario utilizar Internet únicamente con propósitos laborales. Queda terminantemente prohibido a los Usuarios el acceso, la transmisión, distribución, reproducción o almacenamiento de cualquier tipo de información, dato o material que viole esta Política.

b) Es responsabilidad del Usuario evitar la descarga de archivos desde el Internet. Antes de realizar una descarga desde Internet, el Usuario deberá solicitar por medio del Departamento de Tecnologías de Información el software que requiere, y sólo en caso de que no esté disponible o no se cuente con uno similar, deberá solicitarle a su Jefe inmediato que lo solicite ante la UACI, siempre y cuando se haya presupuestado en el Plan Anual de Compras Institucionales, o bien tenga la autorización del Titular o la Secretaría General con la debida justificación técnica avalada por el Departamento de Tecnologías de Información.

c) Queda terminantemente prohibido a los Usuarios el acceso a Internet por medio de dispositivos o servidores que no sean de la PDDH, tales como Módems, USB, Accesos inalámbricos o redes externas, o por medio de otros proveedores cuando esté haciendo uso de la red de la PDDH.

d) Queda terminantemente prohibido a los Usuarios no autorizados interferir o tratar de interferir con los servicios Internet de la PDDH o de cualquier otro servidor de Internet, aun cuando no pertenezca a la PDDH.

e) Es responsabilidad de los Usuarios desconectarse inmediatamente de páginas de Internet que tengan contenido ofensivo, ya sea sexual, pornográfico, político, racista o de cualquier otro tipo. Los Usuarios que accidentalmente se conecten a estas páginas deberán informar a su superior inmediato, quien deberá comunicarse con el personal técnico que monitorea la Seguridad de la Red para bloquear estos accesos.

f) Es responsabilidad del Jefe del Departamento de Tecnologías de Información, autorizar o denegar el acceso a Internet, de forma temporal o permanente y acorde al perfil del cargo del solicitante. Dicho acceso deberá ser solicitado por medio del procedimiento correspondiente y se otorgará (si procede) previa aprobación del Titular o la Titular o en su defecto a la Secretaría General.

DE LA ADQUISICIÓN DE HARDWARE Y SOFTWARE

a) El proceso de adquisición de Hardware y Software de misión crítica o prioritaria a través de terceros debe cumplir la metodología de adquisición legal y formal de la PDDH e incluir la suscripción de un contrato proforma con cláusulas básicas para la protección de la Información y del Software, así como para documentación y respaldo, con el propósito de proteger los intereses institucionales frente a las cláusulas propuestas por el fabricante, distribuidor o vendedor.

b) La adquisición de Hardware y Software, o el desarrollo de programas, sólo se gestionará únicamente a través de la Jefatura del Departamento de Tecnologías de Información, quién garantizará la compatibilidad de los sistemas operativos, los requisitos de conectividad a la Red, entre otros.

c) A menos que se indique lo contrario, los Usuarios deben asumir que todo el Software de la PDDH está protegido por la Legislación sobre Derechos de Autor y requiere Licencia de Uso.

Por tal razón, es ilegal y queda terminantemente prohibido a los Usuarios hacer copias o usar el Software para fines personales.

d) Queda terminantemente prohibido a los usuarios utilizar software descargado desde Internet; y en general, software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por la Jefatura del Departamento de Tecnologías de Información, en los términos relativos al uso de internet de la presente política

DE LOS DISPOSITIVOS MÓVILES (LAPTOP).

a) Se prohíbe tener como herramientas de trabajo, computadores portátiles (laptops), CPU's, USB´s o cualquier otro equipo de propiedad del usuario, salvo autorización previa emitida por el jefe de mayor jerarquía del área que corresponda y el correspondiente registro en la TI en el departamento de Activo Fijo de la PDDH.

b) Es responsabilidad del Usuario utilizar los CD/DVD, dispositivos de memoria USB´s, etcétera, de manera adecuada. Queda terminantemente prohibido al Usuario usar en los equipos de la PDDH, CD/DVD, USB u otros dispositivos de almacenamiento que previamente hayan sido utilizados en computadores de uso público o dudoso, como, por ejemplo: centros educativos, ciber café, o incluso, su computador personal sin la debida revisión por parte del antivirus corporativo.

c) Es responsabilidad del Usuario que usa una Laptop de la PDDH o personal proteger la información propiedad de la PDDH guardada o archivada en el mismo, para lo cual deberá cumplir las siguientes reglas básicas:

- No dejar la Laptop desatendida en lugares públicos para evitar que el equipo o la información sea sustraída.
- Cifrar el contenido de la Laptop para evitar el acceso a los datos en caso de que el equipo sea objeto de robo.
- Usar contraseñas robustas, en lo posible con encriptación para evitar el acceso no autorizado a datos importantes.
- Respaldar la información antes de viajar.
- No desensamblar la Laptop. Sólo un representante técnico autorizado por el fabricante podrá dar servicio y reparar la computadora.

d) Toda laptop perteneciente a la PDDH debe tener instalado el software oficial de antivirus y de ser posible el cifrado del disco para evitar el acceso a los datos en caso de que sea objeto de pérdida o robo.

e) Es obligatorio para todo el personal que usa dispositivos inalámbricos, propiedad de la PDDH, para el desarrollo de sus funciones, como: teléfonos celulares, ipad, ipod, etc. Que utilice como mecanismo de seguridad el bloqueo automático de los mismos y el uso de contraseña de acceso, caso contrario se aplicarán las sanciones correspondientes.

f) Es responsabilidad del usuario, realizar un respaldo periódico de la información contenida en los dispositivos móviles o portátiles asignados, para evitar la pérdida de dicha información por robo, extravío, daño del aparato o cualquier otra circunstancia.

g) Es responsabilidad del Usuario que usa una Laptop de la PDDH, proteger la información guardada o archivada en la misma, para lo cual deberá cumplir las siguientes normas:

- Utilizar un candado físico para anclar la Laptop cuando vaya a ausentarse temporalmente.
- Eliminar datos innecesarios que puedan estar almacenados en la Laptop.
- Guardar todos los detalles del computador, incluyendo fabricante, modelo y número serial para poder llenar formularios en caso de ser necesitados.
- Asegurarse de apagar la Laptop, no dejarla en modo hibernación ni suspenso (stand-by) antes de empacarla.
- No empacar la Laptop dentro de un portafolio o valija que se encuentre densamente cargada con otros objetos. La compresión podría ocasionar un daño interno a ésta.
- No rayar, flexionar, golpear, o presionar la superficie de la pantalla de cristal líquido (LCD) de la Laptop.
- No colocar ningún objeto entre la pantalla y el teclado. No levantar la computadora deteniéndola por la pantalla únicamente. Cuando se levante la Laptop abierta, detenerla a por la mitad inferior.
- No voltear la Laptop sobre si misma mientras el adaptador de corriente está conectado. Esto podría romper su conector.
- No fijar la Laptop dentro de un vehículo o en cualquier otro lugar que esté sujeto a vibraciones continuas.

- No tocar el lente dentro de la bandeja de la unidad de DVD/CD-ROM. El disco compacto deberá de sostenerse por las orillas y no deberá tocarse la superficie de este.

DE LA CONTRATACIÓN DE CONSULTORES DE SERVICIOS TECNOLOGICOS

a) No se deberá contratar a consultores para servicios que puedan crear conflicto con sus obligaciones previas o vigentes con respecto a los intereses de la PDDH, o cuando el juicio profesional, objetividad, imparcialidad o la defensa del interés institucional se puedan ver afectados por consideraciones personales, de índole financiera u otra.

b) La PDDH exige a todos los Consultores, observar los más altos niveles éticos y cualquier empleado está obligado a denunciar ante las instancias correspondientes, todo acto sospechoso de fraude o corrupción del cual tenga conocimiento o sea informado durante el proceso de selección y las negociaciones o la ejecución de un contrato.

c) Todo contrato celebrado con terceros deberá contener cláusulas de confidencialidad e incluir al menos los siguientes puntos: acuerdo de no divulgación total o parcial de la información, propiedad de la información y vigencia perenne del acuerdo, responsabilidades de las partes y límite de uso de la información, siendo responsable el titular del área ejecutora, de vigilar su estricto cumplimiento.

DE LA SEGURIDAD FÍSICA

a) Todos los sitios donde se encuentren sistemas de procesamiento de información (manejo de datos electrónicos) o de almacenamiento, así como el acceso a las diferentes oficinas, deben de ser protegidos contra accesos no autorizados, utilizando procedimientos o tecnologías de autenticación, monitoreo y registro.

b) En aquellas oficinas en donde existen empleados con acceso al lugar o los equipos de comunicación hacia las redes de datos o telefonía de la PDDH, el jefe del departamento, unidad o delegado departamental deberá tomar las medidas pertinentes para el resguardo y cuidados especiales del equipo.

DE LA SEGURIDAD APLICABLE A LAS BITACORAS (LOGS)

a) Es responsabilidad del Jefe de la Unidad Técnica de Informática asegurar que se generen Logs o Bitácoras para los equipos y aplicaciones clasificadas como críticas, así como los

solicitados por el área de Auditoría; dichos Logs deben ser custodiados en forma segura para evitar su modificación.

b) Los Logs o bitácoras generadas deben ser monitoreados periódicamente para detección temprana de posibles fallas en los equipos y aplicaciones o vulnerabilidades de seguridad. Esta supervisión será en primer lugar por la Unidad Técnica de Informática, Administrador de la Seguridad de la Información, Unidad de Auditoría Interna a través del Auditor de Sistemas de Información.

DE SEGURIDAD DE APLICACIÓN ESPECÍFICA

AREA DE TECNOLOGÍAS DE INFORMACIÓN (SISTEMAS).

DE LA SEGURIDAD DE SERVIDORES

a) Es responsabilidad de la Jefatura de Departamento de Tecnologías de Información de la PDDH, asignar a todos los servidores internos instalados en la institución, un responsable por la administración del sistema de cada uno y contar como mínimo con la siguiente información relacionada:

- Nombre del Servidor
- Localización del Servidor
- Nombre del administrador responsable y localización al igual que su suplente
- Detalle especifico del Hardware
- Sistema operativo y su versión
- Aplicaciones y bases de datos
- Función principal y/o uso
- Acuerdos de mantenimiento (Plan detallado – Cronograma)

b) Es responsabilidad de cada administrador del sistema, que todos los servidores, así como su sistema operativo, tengan estándares de configuración de seguridad documentados y aplicados de acuerdo al rol del servidor en la organización.

c) Es responsabilidad del Administrador de Sistemas de la UTI, que las actualizaciones más recientes de seguridad sean instaladas en los servidores tan pronto como sea posible, validando previamente en ambientes de prueba, considerando el menor impacto en la continuidad de los servicios que se prestan a los usuarios internos y contando con la

aprobación de la Jefatura de Tecnologías de Información. Dicha actualización será producto de revisiones mensuales a las publicaciones de seguridad del emisor del software.

d) Es responsabilidad de la Jefatura de Tecnologías de Información, definir los procesos tecnológicos, mantenerlos actualizados y velar por su cumplimiento, para mantener los servidores protegidos físicamente en un ambiente con control de acceso y protección ambiental.

e) Es responsabilidad de la Jefatura de Tecnologías de Información de la PDDH garantizar que los cambios que se hagan tanto a hardware como software en ambiente de producción cuenten con la aprobación respectiva.

f) Es responsabilidad de la Jefatura de Tecnologías de Información reportar a su Jefe Inmediato con copia al Administrador de Seguridad de la Información, violaciones a las configuraciones, hechas por los usuarios, de acuerdo con las políticas definidas para servidores y estaciones de trabajo.

DE LA SEGURIDAD DE EQUIPOS DE COMUNICACIÓN

a) Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación, video seguridad y cómputo deben ser tratadas como Información Confidencial.

b) Es responsabilidad de la Jefatura de Tecnologías de Información de la PDDH, definir los procesos de su área, mantenerlos actualizados y velar por su cumplimiento, para que todos los recursos de red críticos como enlaces de comunicaciones, Firewalls, servidores, centrales de conexión o centros de cableado de la institución, estén en áreas de acceso físico restringido.

c) Queda terminantemente prohibido que los empleados y funcionarios de la PDDH lleven a cabo algún tipo de instalación de líneas telefónicas digitales o análogas, canales de transmisión de datos, módems o cambiar su configuración, esto es responsabilidad exclusiva del Departamento de Tecnologías de Información o de cualquier empresa que se haya contratado para tal fin, en cuyo caso será supervisada por la Jefatura de Tecnologías de Información.

d) Es responsabilidad de los responsables del soporte técnicos que haya designado la Jefatura del Departamento de Tecnologías de Información, llevar control estricto y actualizado de la

topología, archivos y parámetros de configuración de la red; así como el inventario de equipos y software de la misma, debiendo guardar una copia de éstos en la Jefatura del Departamento TI.

e) Es responsabilidad del responsable del Área de Desarrollo del Departamento de Tecnologías de Información, definir e implantar con aprobación de la Jefatura del Departamento, procedimientos y controles para la realización de cambios sobre la red de datos y telecomunicaciones, teniendo en cuenta que los horarios no impacten negativamente la disponibilidad de los servicios de red críticos.

f) Queda terminantemente prohibida la utilización de herramientas de monitoreo de red, esta actividad está restringida sólo al área de Tecnologías de Información (Data Center de la PDDH), encargados de efectuar el diagnóstico y mantenimiento del funcionamiento de las redes.

g) Para prevenir la intrusión de hackers a través de puertas traseras, está prohibido el uso de módems en PC´s que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado por la Jefatura de Tecnologías de Información de la PDDH. Todas las comunicaciones de datos deben efectuarse a través de la Red Interna.

DE LA SEGURIDAD EN REDES CON TERCEROS

a) Es responsabilidad del Jefe Jefatura de Tecnologías de Información de la PDDH, definir los procesos de conexión con terceros, mantenerlos actualizados y velar por su cumplimiento para que toda conexión entre las redes de la PDDH y redes con terceros cuenten como mínimo con mecanismos de control de acceso lógico, tales como: Firewall, Proxys y DNS.

b) Es responsabilidad del responsable de la Jefatura de Tecnologías de Información o de quién ésta designe de sus equipos técnicos asegurar que los enlaces de comunicación establecidos con terceros estén controlados y contar como mínimo con la siguiente información relacionada:

- Servicios habilitados
- Origen y destino de la conexión.
- Propósito de la conexión.
- Datos del contacto del tercero como: Nombre, teléfono y correo electrónico.

c) Es responsabilidad de la Jefatura de Tecnologías de Información, o de quién ésta designe de sus equipos técnicos que, en los enlaces de comunicaciones establecidas con terceros, se depure el enrutamiento de tal manera que se publiquen únicamente las redes necesarias para el buen funcionamiento de las aplicaciones que utiliza este enlace.

d) Es responsabilidad de la Jefatura de Tecnologías de Información, o de quién ésta designe de sus equipos técnicos, que los eventos que afecten la seguridad de la red privada de la PDDH queden registrados en una bitácora como documento indispensable para posteriores análisis de riesgos.

e) Es responsabilidad de la Jefatura de Tecnologías de Información, o de quién ésta designe de sus equipos técnicos, garantizar comunicaciones encriptadas o cifradas y seguras desde el punto donde se produce al punto donde se consume.

DEL ACCESO Y CONFIGURACIÓN REMOTOS

a) Está prohibido otorgar cuentas o acceso remoto a la red de la PDDH a menos que sea autorizado por de la Jefatura de Tecnologías de Información, o la Secretaría General y sólo a través de VPN's que cuenten con las medidas de seguridad adecuadas.

DE LA SEGURIDAD EN REDES INALÁMBRICAS

a) Es responsabilidad de la Jefatura de Tecnologías de Información, o de quién ésta designe de sus equipos técnicos, observar las siguientes prácticas en la administración de las redes inalámbricas:

- Cambiar la contraseña asignada por el fabricante o de instalación.
- Activar el filtro de direcciones MAC.
- Restringir de acuerdo con lo establecido el número máximo de dispositivos que pueden conectarse.
- Utilizar siempre protocolos de encriptación que estén de acuerdo con los estándares internacionales vigentes, los cuales serán verificados en conjunto con el Administrador de Seguridad de la Información.
- Proporcionar un entorno físicamente seguro a los puntos de acceso.
- Utilizar IPSec, VPN, Firewalls y monitorear los accesos a los puntos de acceso.

- Inhabilitar la emisión Broadcast del SSID.
- Cambiar el SSID (Server Set ID) por defecto de los puntos de acceso, conocidos por todos.

DEL DESARROLLO DE SOFTWARE

a) Es Responsabilidad de la Jefatura del Departamento de Tecnologías de Información de la PDDH, asegurar que todos los sistemas desarrollados por la institución y para la PDDH, cumplan con las Políticas de Seguridad de la Información, y que los contratos con terceros incluyan una cláusula para que éstos se obliguen también a cumplirlas.

b) Con el propósito de garantizar la integridad y confidencialidad de la información que administrará el software desarrollado internamente o por terceros y antes del paso al ambiente de pruebas, es responsabilidad de la Jefatura del Departamento de Tecnologías de Información de la PDDH, garantizar que existen evidencias de que se ejecutan pruebas intrínsecas al desarrollo y a la documentación técnica respectiva.

c) Es Responsabilidad de la Jefatura del Departamento de Tecnologías de Información de la PDDH o de quién ésta designe de sus equipos de soporte técnico establecer los mecanismos para asegurar que solamente las funciones descritas en el documento de especificaciones de la solución tecnológica aprobado sean desarrolladas.

d) Se prohíbe que los Programadores de software conozcan las claves utilizadas en ambientes de producción (encriptares, claves, etc.) y es responsabilidad de la Jefatura del Departamento de Tecnologías de Información de la PDDH asegurar el cumplimiento de dicha restricción.

e) Es Responsabilidad de la Jefatura del Departamento de Tecnologías de Información de la PDDH, garantizar que los desarrollos y/o modificaciones hechos a los sistemas de aplicación, no se trasladen al ambiente de producción, si no se cuenta primero con todos los requerimientos documentados, pruebas de aceptación, manuales de usuario y técnico, Acta de Formalización y firma de aceptación de involucrados, programas fuentes, la documentación de entrenamiento, operación y de seguridad adecuados.

f) Es Responsabilidad de la Jefatura del Departamento de Tecnologías de Información de la PDDH o de quién ésta designe de sus equipos de soporte técnico, definir y mantener actualizados los procesos de desarrollo para que la nueva programación y/o modificaciones

efectuadas a los sistemas de información, cumplan un proceso estricto de pruebas que validen la calidad del Software, antes de ser validados en la etapa de pruebas de aceptación.

DE LOS CENTROS DE CÓMPUTO Y TELECOMUNICACIONES

a) Los Centros de Capacitación, así como los centros de procesamiento de datos (data center) en el uso de las tecnologías de información, también llamados Centros de Cómputo, así como las Áreas de Telecomunicaciones de la PDDH están clasificadas como áreas de acceso restringido, debiendo estar disponibles únicamente para fines de capacitación, formación y asistencia técnica.

b) Es responsabilidad de la Jefatura de las Tecnologías de Información de la PDDH, asegurar que todos los recursos informáticos y telecomunicaciones de la institución, cuenten con planes de mantenimiento preventivo y/o correctivo debidamente contratados.

c) Es responsabilidad de la Jefatura de las Tecnologías de Información de la PDDH, que los Centros de Cómputo y las áreas de telecomunicaciones de la Institución cuenten con sistemas de control de acceso físico, que puedan ser auditados.

DE LOS RESPALDOS

a) La Procuraduría para la Defensa de los Derechos Humanos, deberá contar como mínimo con dos centros u oficinas diferentes, para el almacenamiento de respaldos. Para efecto de las Políticas de Respaldo, se referirá como centro alterno, el situado distante en una bóveda de un banco local contratado para tal efecto.

b) Es responsabilidad de la Jefatura de las Tecnologías de Información de la PDDH o de quién ésta designe, nombrar o delegar a un Administrador de Seguridad de las tecnologías de Información, quién debe definir, documentar, mantener y probar un proceso de respaldo y recuperación para todos los datos de producción independientemente del servidor en el Data Center donde se encuentre, el que debe cumplir con las siguientes reglas:

- Periodicidad: Diaria
- Tipo de Respaldo: Incremental/Total dependiendo de la viabilidad
- Retención: 5 años
- Custodia: En centro alterno de almacenamiento
- Prueba de Recuperación: Cada seis meses

c) Es responsabilidad del Administrador de Seguridad de las tecnologías de información definir, documentar, mantener y probar un proceso de respaldo y recuperación para a todos los archivos de aplicaciones de producción independientemente del servidor en el Data Center donde se encuentre y deben cumplir con las siguientes reglas:

- Periodicidad: Semanal
- Tipo de Respaldo: Total
- Retención: 5 años (de acuerdo a los lineamientos de la Ley de Transparencia y Acceso a la Información Pública)
- Custodia: En centro alterno de almacenamiento
- Prueba de Recuperación: Cada seis meses

d) Es responsabilidad del Administrador de las tecnologías de información, definir, documentar, mantener y probar un proceso de respaldo y recuperación para todas las Configuraciones de los servidores incluyendo los elementos de comunicaciones y seguridad de producción, que estén en el Data Center y deben cumplir con las siguientes reglas:

- Periodicidad: Semanal
- Tipo de Respaldo: Total
- Retención: 1 año
- Custodia: En centro alterno de almacenamiento
- Prueba de Recuperación: Cada seis meses

e) Es responsabilidad del Administrador de las tecnologías de información, definir, documentar, mantener y probar un proceso de respaldo y recuperación para todas las imágenes y documentos digitalizados de producción independientemente del servidor en el Data Center donde se encuentre y deben cumplir con las siguientes reglas:

- Periodicidad: Diaria
- Tipo de Respaldo: Incremental
- Retención: 10 años
- Custodia: En centro alterno de almacenamiento
- Prueba de Recuperación: Cada seis meses

f) Es responsabilidad del Administrador de las tecnologías de información, definir, documentar, mantener y probar un proceso de respaldo y recuperación para todos los logs o bitácoras transaccionales del ambiente de producción independientemente del servidor en el Data Center donde se encuentre y deben cumplir con las siguientes reglas:

- Periodicidad: Semanal
- Tipo de Respaldo: Incremental
- Retención: 5 años
- Custodia: En centro alterno de almacenamiento
- Prueba de Recuperación: Cada un año
- Campos mínimos requeridos en el archivo de logs:
  - ✓ Persona
  - ✓ Lugar
  - ✓ Tiempo
  - ✓ Acción

g) Es responsabilidad del Administrador de las tecnologías de información, definir, documentar, mantener y probar un proceso de respaldo y recuperación para todos los logs de consulta de producción independientemente del servidor en el Data Center donde se encuentre y deben cumplir con las siguientes reglas:

- Periodicidad: Semanal
- Tipo de Respaldo: Incremental
- Retención: 6 meses
- Custodia: En centro alterno de almacenamiento
- Prueba de Recuperación: Cada un año

h) Es responsabilidad del responsable del Área de Desarrollo de sistemas definir, documentar, mantener y probar un proceso de respaldo y recuperación para todos los archivos de programación del ambiente de Desarrollo independientemente del servidor en el Data Center donde se encuentre y deben cumplir con las siguientes reglas:

- Periodicidad: Diaria
- Tipo de Respaldo: Total
- Retención: 1 año
- Custodia: En centro alterno de almacenamiento

i) Es responsabilidad del Operador de Cierres ejecutar y monitorear la realización de los procesos de respaldo asociados con las políticas de respaldo de la a) a la h).

j) Es responsabilidad del Coordinador de Telecomunicaciones, custodiar los respaldos generados acorde con las políticas de respaldo de la a) a la h).

k) Es responsabilidad del Coordinador de Telecomunicaciones, garantizar que el sitio alterno de almacenamiento cuente como mínimo con lo siguiente:

- Debe estar localizado en un lugar distante y distinto en donde se generó la copia de la información original.
- No debe estar en una zona con peligro de derrumbe o inundación.
- Control ambiental apropiado para el almacenamiento de los dispositivos utilizados para respaldar la información.
- Control de acceso físico
- Control de Inventario actualizado.
- Transporte seguro de la información respaldada
- Encriptación del contenido de los dispositivos de almacenamiento a resguardar.

Es responsabilidad de la Jefatura del Departamento de Tecnologías de Información o de quién ésta haya designado como Coordinador de Telecomunicaciones y las Redes de Datos, de la PDDH, que los equipos de almacenamiento o respaldo de información que deban ser desechados, se destruyan físicamente o sean escritos de manera segura a través del uso de herramientas especiales que garanticen y verifiquen que no queda información remanente