"AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN Y LA IMPUNIDAD"

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN

HUÁNUCO - PERÚ

SECRETARIA GENERAL

RESOLUCIÓN CONSEJO UNIVERSITARIO N° 0328-2019-UNHEVAL

Cayhuayna, 15 de enero de 2019.

VISTOS, los documentos que se acompañan en cincuenta y nueve (59) folios y;

CONSIDERANDO:

Que el Jefe de la Unidad de Informática, mediante Oficio N° 120-2018-UNHEVAL/UI, de fecha 20.DIC.2018, remite para su aprobación los siguientes documentos:

1. Lineamientos de las Políticas de Seguridad Informática de la Universidad Nacional Hermilio Valdizán de Huánuco.
2. Plan Estratégico de Gobierno Electrónico 2018-2020 de la Universidad Nacional Hermilio Valdizán de Huánuco.
3. Plan Estratégico de Tecnologías de la Información 2018-2020 de la Universidad Nacional Hermilio Valdizán de Huánuco.

Que el Rector remite el caso a Secretaría General, con el Proveído N° 049-2019-UNHEVAL-CU/R, para que se emita la resolución correspondiente;

Que el Presidente de la Comisión Consultiva de la Alta Dirección, mediante Oficio N° 316-2018.-UNHEVAL-CCAD, de fecha 27.DIC.2018, luego de haber revisado cada uno de los documentos opina por la aprobación del Plan Estratégico de Gobierno Electrónico 2018-2019; el Estratégico de Gobierno Electrónico 2018-2020 de la Universidad Nacional Hermilio Valdizán de Huánuco y los lineamientos de las políticas de Seguridad Informática;

Que en la sesión extraordinaria N° 21 de Consejo Universitario, del 03.ENE.2019, con la opinión favorable de la Comisión Consultiva de la Alta Dirección, y en mérito a lo establecido en el inciso b), del Artículo N° 113 del Estatuto de la UNHEVAL, y el inciso b), del Art. 155° del Reglamento General de la UNHEVAL, el pleno acordó aprobar los siguientes documentos elaborados por la Unidad de Informática, de la Dirección General de Administración:

1. Lineamientos de las Políticas de Seguridad Informática de la Universidad Nacional Hermilio Valdizán de Huánuco.
2. Plan Estratégico de Gobierno Electrónico 2018-2020 de la Universidad Nacional Hermilio Valdizán de Huánuco.
3. Plan Estratégico de Tecnologías de la Información 2018-2020 de la Universidad Nacional Hermilio Valdizán de Huánuco.

Que el Rector remite el caso a Secretaría General, con el Proveído N° 049-2019-UNHEVAL-CU/R, para que se emita la resolución correspondiente.

Estando a las atribuciones conferidas al Rector por la Ley Universitaria N° 30220, por el Estatuto y el Reglamento de la UNHEVAL, la Resolución N° 050-2016-UNHEVAL-CEU, del 26.AGO.2016, del Comité Electoral Universitario, que proclamó y acreditó, a partir del 02.SET.2016 hasta el 01.SET.2021, a los representantes de la Alta Dirección; por la Resolución N° 2780-2016-SUNEDU-02-15.02, del 14.OCT.2016, que resolvió proceder a la inscripción de las firmas de las autoridades de la UNHEVAL en el Registro de Firma de Autoridades Universitarias, Instituciones y Escuelas de Educación Superior de la SUNEDU; y estando a lo dispuesto en la Resolución Rectoral N° 0016-2019-UNHEVAL, que encarga las funciones de Secretario General al Lic. Humberto RIQUELME LUNA, desde el 10 hasta el 17.ENE.2019, mientras dure la ausencia de la Titular;

SE RESUELVE:

1°. **APROBAR** los siguientes documentos elaborados por la Unidad de Informática, de la Dirección General de Administración, por lo expuesto en los considerandos precedentes::

1.1 Lineamientos de las Políticas de Seguridad Informática de la Universidad Nacional Hermilio Valdizán de Huánuco.

1.2 Plan Estratégico de Gobierno Electrónico 2018-2020 de la Universidad Nacional Hermilio Valdizán de Huánuco.

1.3 Plan Estratégico de Tecnologías de la Información 2018-2020 de la Universidad Nacional Hermilio Valdizán de Huánuco.

2°. **DISPONER** que la Unidad de Informática adopte las acciones complementarias.

3°. **DAR A CONOCER** la presente Resolución a los órganos competentes.

Regístrese, comuníquese y archívese.

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN RECTOR HUÁNUCO

Dr. Reynaldo M. OSTOS MIRAVAL
RECTOR

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN SECRETARÍA GENERAL HUÁNUCO

Lic. Humberto RIQUELME LUNA
SECRETARIO GENERAL (E)

...que transcribo a UD. para su conocimiento y demás fines
Abog. Yercely Karin Figueroa Quiñone
SECRETARIA GENERAL

UNIVERSIDAD NACIONAL HERMILIO VALDIZÁN - HUÁNUCO
PORTAL DE TRANSPARENCIA
RECIBIDO
17 ENE. 2019
N° Registro: ....
Hora: .... Firma: ....

Distribución:
Rectorado
VRAcad
VRInv
OCI.
AL
Transparencia
DCalidad
UI
DPLAN
JPPTO
Facultades (14)
DIGA
RRHH
Archivo

UNIVERSIDAD NACIONAL
HERMILIO VALDIZÁN

LINEAMIENTOS DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

Huánuco - Perú

CONTENIDO

1. INTRODUCCIÓN

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las instituciones y/o empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información. Estos riesgos a los que se enfrentan ha llevado a que se desarrolle un documento de directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la Institución.

En este sentido, las políticas de seguridad informática definidas partiendo desde el análisis de los riesgos a los que se encuentra propensa la Universidad, surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten crecer y mantenerse competitiva a la Institución. Ante esta situación, el proponer nuestra política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades en su aplicación, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea a la Institución.

Cada política de seguridad informática es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos, así como motor de intercambio y desarrollo en el ámbito de sus funciones. Tal invitación debe concluir en una posición consciente y vigilante del personal respecto al uso y limitaciones de los recursos y servicios informáticos críticos de la Institución.

El presente es una propuesta de las políticas de seguridad informática, elaborado por la Unidad de Informática, y contiene los puntos importantes y acciones necesarias para normar en la prevención y contingencias relacionadas con las tecnologías de información institucional. Esta ha sido debidamente analizada, revisada y planteada, de tal manera que muestra una buena forma de operar el sistema con seguridad, respetando en todo momento las normas y reglamentos vigentes de la Institución.

2. ALCANCE

Todo el personal académico, administrativo, alumnos, proveedores y demás personas relacionadas con nuestra institución y que hagan uso de nuestros servicios e infraestructura de cómputo y comunicaciones, deben de dar cumplimiento a los Lineamientos de Seguridad Informática Institucional; tanto en el interior de las instalaciones del Campus Universitario, como en el exterior; de manera física y lógica vía internet.

3. FINALIDAD

Desarrollar un sistema de seguridad, el cual significa planear, organizar, dirigir y controlar las actividades que se realizan; para que de esta manera se pueda mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la Institución.

Se debe considerar que las políticas de seguridad informática, por si solas no constituyen una garantía para la seguridad informática, sino que depende principalmente del esfuerzo de todo el personal que labora en la organización, el de velar por su cumplimiento.

4. MARCO LEGAL

Dentro de las normas legales relacionadas con el tema de políticas de Seguridad de la Información y de Comunicaciones que rigen para el sector público, se consideran a las siguientes:

- Ley Nº 27309, título V capítulo X del código Penal y que trata sobre los "Delitos Informáticos".

- Ley Nº 27815, ley del código de Ética de la Función Pública.

- Resolución Ministerial Nº 246-2007-PCM. Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

- Resolución Ministerial Nº 129-2012-PCM. Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP-ISO-IEC-27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad Sistemas de gestión de seguridad de la información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.

5. ORGANIZACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

5.1. PERSONAS

Los funcionarios y la seguridad informática

La responsabilidad por la seguridad de la información no sólo corresponde a la Unidad de Informática, sino que es una obligación de cada funcionario y/o colaborador de la Institución.

5.1.1. Códigos de identificación y claves

a. Los mecanismos de acceso que les sean otorgados a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona, a menos que exista un requerimiento legal o medie un procedimiento de custodia de llaves. De acuerdo con lo anterior, los usuarios no deben obtener las claves u otros mecanismos de acceso de otros usuarios que pueda permitirles un acceso indebido.

b. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de usuario y clave personal.

5.1.2. Control de la Información

a. Los usuarios deben informar inmediatamente a la Unidad de Informática toda vulnerabilidad encontrada en los sistemas, aparición de virus o programas sospechosos e intentos de intromisión, y no deben distribuir este tipo de información interna o externamente.

b. Los usuarios no deben instalar software en sus computadoras o en los servidores sin la debida autorización.

c. Los usuarios no deben intentar sobrepasar los controles de los sistemas, examinar las computadoras y redes de la universidad en busca de archivos de otros sin su autorización o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas.

d. Los funcionarios y/o trabajadores no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas. Esto incluye los controles del sistema de información y su respectiva implementación.

e. Los funcionarios y/o trabajadores no deben destruir, copiar o distribuir los archivos de la universidad sin los permisos respectivos.

f. Todo funcionario y/o trabajador que utilice los recursos de los sistemas tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información ha sido clasificada como crítica.

5.1.3. Otros usos

Las computadoras, sistemas y otros equipos deben usarse sólo para las actividades propias de la entidad, por lo tanto, los usuarios no deben usar sus equipos para asuntos personales.

5.2. SOFTWARE

Los funcionarios y/o trabajadores con funciones y responsabilidades para con el software institucional deben seguir los siguientes lineamientos para proteger este activo y la información que a través de él se maneje.

5.2.1. Administración del Software

a. La universidad debe contar en todo momento con un inventario actualizado del software de su propiedad como el comprado a terceros, desarrollado internamente o el adquirido bajo licenciamiento. Las licencias se almacenarán bajo los adecuados niveles de seguridad. Igualmente, todo el software y la

documentación del mismo que posea la universidad incluirán avisos de derechos de autor y propiedad intelectual.

b. En todos los equipos de cómputo de la Institución, solo se permite la instalación de software con licenciamiento vigente, ya sea de uso libre o comercial. El área de Soporte Técnico está facultada para asesorar en la instalación del software.

c. Toda persona que necesite adquirir software, podrá solicitar apoyo a la Unidad de Informática, quien verificará los requerimientos técnicos y el completo licenciamiento, y recabar una copia de esta licencia para su resguardo.

d. Todo empleado, alumno y terceros que instale software sin licenciamiento vigente o malicioso en equipos de cómputo de la institución, se hace único responsable de las consecuencias que esto conlleve.

e. Las licencias de uso de software propiedad de la Universidad, otorgan a éste el derecho de emplearlas exclusivamente en los equipos asignados al personal de la institución.

f. Todas las aplicaciones se clasificarán en una de las siguientes categorías: Crítica, Prioritaria y Requerida. Para las críticas y prioritarias deberá permanecer una copia actualizada y su documentación técnica respectiva, como mínimo en un sitio alterno y seguro.

g. Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad. Los programas que se encuentren en el ambiente de producción de la universidad, se modificarán únicamente por el personal autorizado, de acuerdo con los procedimientos internos establecidos y se considerarán planes de contingencia y recuperación.

h. Los servidores públicos no pueden escribir, ingresar o usar ningún software a menos que esto haya sido autorizado y aprobado por la Unidad de Informática.

i. Para evitar dudas, se prohíbe el uso del software que se enlista a continuación, a menos que se cuente con la autorización explícita de la Unidad de Informática para circunstancias específicas:

- ✓ Software de juegos y recreación de cualquier tipo.
- ✓ Cualquier software no autorizado que haya sido obtenido de Internet.
- ✓ Software no solicitado sin importar de que fuente provenga.
- ✓ Software creado por un empleado actuando como individuo y que no haya sido aprobado por la Unidad de Informática.
- ✓ Copias sin licencia de software autorizado.

j. Todo uso y administración del software comprado debe ser acorde con los contratos de licencia y copyright respectivos.

k. Deben guardarse las copias maestras del software y sus licencias en lugar seguro y tenerlas disponibles para su inspección si fuera necesario.

l. La administración debe garantizar que el software haya sido probado adecuadamente antes de confiarle el procesamiento de las operaciones a las diferentes áreas de la Institución.

m. Deben aplicarse los parches de seguridad más recientes con los que cuente el proveedor del software.

5.2.2. Control antivirus

Debe utilizarse un sistema estándar de detección de virus actualizado de la Institución, automáticamente para:

a. Escanear todos los archivos que ingresen en el entorno informático de la Institución vía e- mail, cualquier tipo de dispositivo de almacenamiento u otra fuente externa tal como el Internet; para identificar, informar y, si se considera necesario, eliminar virus informáticos en la primera oportunidad que se tenga.

b. Escanear y, si fuera necesario, corregir o mantener en cuarentena todos los archivos enviados desde la Institución a los usuarios, proveedores y otras contrapartes externas por e-mail u otros medios para asegurarse de que no se esté distribuyendo virus sin saberlo.

c. Actualizar las definiciones antivirus por lo menos una vez a la semana.

d. Ejecutar por lo menos una vez a la semana el análisis antivirus en los equipos de cómputo de la Institución.

e. El usuario no deberá desinstalar el software antivirus de su computadora, pues ocasionaría un riesgo de seguridad ante el peligro de virus.

f. Las carpetas compartidas, dentro de una Red, deben tener una clave de acceso, la misma que podría ser cambiada periódicamente, de acuerdo al tipo de información que se comparta.

g. El correo electrónico es el medio de transmisión preferido por los virus, por lo que hay que tener especial cuidado en su utilización.

h. No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca parches de seguridad, atractivos premios o temas provocativos.

i. Verificar cualquier software que haya sido instalado, asegurándose que provenga de fuentes conocidas y seguras.

j. No instalar productos que se descargan de Internet, ya que son una potencial vía de propagación de virus.

k. Evitar ejecutar o abrir archivo con doble extensión.

l. Si el antivirus detecta un archivo infectado que no puede ser reparado, entonces debe ser eliminado.

m. Realizar respaldos de seguridad de la PC al menos una vez por mes.

5.2.3. Desarrollo, pruebas, implantación y mantenimiento de Software

Desarrollo

a. La universidad deberá tener una metodología formal para el desarrollo de software las cuales cumplirán con las políticas, normas, procedimientos, controles y otros estándares aplicables en el desarrollo de sistemas.

b. Con el propósito de garantizar integridad y confidencialidad de la información que administrará el software desarrollado y antes del paso a los operadores finales, se deberán ejecutar las pruebas intrínsecas al desarrollo y a la documentación técnica respectiva.

c. Los desarrollos y/o modificaciones hechos a los sistemas de aplicación no deberán trasladarse a los operadores finales si no se cuenta primero con la adecuada documentación de operación y de seguridad.

Pruebas

a. El área de desarrollo de sistemas, debe entregar el software desarrollado con los códigos fuente a la unidad encargada de realizar las pruebas en cuanto a: código mal intencionado y debilidades de seguridad; cabe mencionar que para realizar dicho procedimiento es preferible que se utilicen herramientas automáticas.

b. Para garantizar la integridad de la información que se maneja en el área de operaciones, las pruebas deberán ser planeadas, ejecutadas, documentadas y controladas a nivel de sus resultados. Cabe mencionar que el ambiente de pruebas deberá ser lo más idéntico, en su configuración, al ambiente real de operación.

c. Las pruebas sobre el software desarrollado deberán contemplar aspectos funcionales, de seguridad y técnicos. Además, se incluirá una revisión exhaustiva a la documentación mínima requerida.

d. Se deberá poseer un cronograma para la ejecución de las pruebas con el fin de cumplir con los compromisos institucionales acordados. Éste podrá verse afectado en su calendarización por aquellos eventos en que se tengan que atender desarrollos rápidos únicamente por exigencias mandatorias de entes superiores.

Implantación

a. Para implantar un software debe mediar una autorización por escrito del responsable para tal fin. Las características que son innecesarias en el ambiente informático se identificarán y desactivarán en el momento de la instalación del software.

b. Antes de implementar el software en determinada área, se verificará que se haya realizado la divulgación y entrega de la documentación, la capacitación al personal involucrado, su licenciamiento y los ajustes de parámetros en el área donde será operado. Es necesario que exista un cronograma de puesta en operación del software, con el fin de minimizar el impacto del mismo.

c. Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el personal especializado para tal efecto.

d. Los programas en el ambiente de producción serán modificados únicamente por personal autorizado y cuando se requiera por fuerza mayor de acuerdo con las normas institucionales establecidas.

Mantenimiento

a. La sub unidad de desarrollo de sistemas no hará cambios al software en operación sin las debidas autorizaciones por escrito y sin cumplir con los procedimientos establecidos. Así mismo, se

contará con un procedimiento de control de cambios que garantice que sólo se realicen las modificaciones autorizadas.

b. La documentación de todos los cambios hechos al software se realizará simultáneamente con el proceso de cambio. Se deberá considerar, además, que cuando un tercero efectúe algún ajuste al software, éste deberá firmar un acuerdo de no divulgación y utilización no autorizada del mismo.

c. El procedimiento para realizar el mantenimiento debe tener en cuenta los tiempos de respuesta máximos que se pueden permitir ante situaciones de no funcionamiento del software.

5.2.4. Servicios informáticos en la RED

a. Todo personal, alumnos y terceros son responsables del buen uso de los servicios informáticos institucionales alojados en nuestras instalaciones y en la nube, asignados para realizar sus funciones administrativas y académicas.

b. El personal de la Unidad de Informática queda facultado para acceder a los equipos de cómputo institucionales, aun en aquellos que no están a su resguardo, para la realización de revisiones en base al cumplimiento de medidas de seguridad informática tales como el software antivirus, actualizaciones, entre otros.

c. El jefe del área que administra los sistemas de información, es responsable de autorizar el nivel de acceso con privilegios mínimos necesarios para que el personal académico y administrativo realice sus funciones.

d. Ninguna persona debe ver, copiar, alterar o destruir la información que reside en los equipos de cómputo y servidores sin el consentimiento explícito del responsable del equipo o del dueño de la información.

e. Todas las cuentas de usuario y su respectiva contraseña de acceso a los sistemas y servicios de información en la RED de la Universidad, son personales, permitiéndose el uso bajo su

responsabilidad, única y exclusivamente durante la vigencia de los derechos del usuario. La vigencia de las cuentas de usuarios es facultad de la Unidad de Informática y del área dueña del servicio, éstas son habilitadas, suspendidas o canceladas por el área en consideración a las solicitudes, necesidades y conductas de los usuarios.

f. Todo hardware de telecomunicaciones (switches, enrutadores, puntos de acceso inalámbrico, entre otros) y servidores (web, FTP, correo y otros) que se requiera habilitar en la red de telecomunicaciones institucional debe ser previamente autorizado por la Unidad de Informática.

g. A todo equipo de cómputo institucional conectado a la RED de la Universidad (computadoras de escritorio y portátiles), personal autorizado por la Unidad de Informática deberá de configurarlo en la RED de dominio de la Universidad.

h. A toda persona que deje de laborar o tener relación con la Universidad, le será cancelado su acceso de manera definitiva a los recursos informáticos institucionales. La Oficina de Gestión de Recursos Humanos comunicará a la Unidad de Informática toda alta, baja o cambio del personal para que se tomen las medidas correspondientes de privilegios de acceso a los servicios de red.

5.2.5. Uso de Internet

a. El servicio de Internet a través de las redes institucionales se considera como herramienta de trabajo, por lo que todo usuario deberá utilizarlo exclusivamente para apoyo a sus actividades académicas y/o administrativas en la Universidad.

b. El personal responsable del Área de Redes y Telecomunicaciones de la Unidad de Informática puede restringir de forma parcial o total el acceso a Internet para el personal de la institución, considerando para ello las funciones laborales que éstos realizan.

c. Todo usuario que descargue información y archivos de Internet mediante el navegador web u otro medio, debe de omitir descargar archivos de dudosa procedencia. Los archivos descargados de Internet pueden contener virus o software malicioso que pongan en riesgo la información del equipo de cómputo de la persona, e incluso al de la Institución.

d. Está prohibida la navegación en sitios de contenido pornográfico, juegos, chats, ocio y todo aquellos que no sea justificable para el buen desempeño de las labores del personal de la institución.

e. El Área de Redes y Telecomunicaciones de la Unidad de Informática inhabilitará todas las direcciones de Internet que cumplan con lo expuesto en el punto anterior.

f. No debe transmitirse información confidencial o referida a valores a través de la Internet sin antes aplicar controles adicionales (por ejemplo, el cifrado).

g. Todo servidor debe ejecutar sólo los procesos mínimos necesarios para llevar a cabo sus funciones. Mismos que serán notificados por parte del responsable del equipo para poder adecuar los controles de acceso al mismo.

h. La operación de controles de firewall debe estar sujeta a pruebas con regularidad, así como a monitoreo automatizado.

i. Deben implementarse herramientas automatizadas para prevenir la recepción de códigos ejecutables provenientes de la Internet que pudieran representar una amenaza para la seguridad informática de la Institución.

5.3. DATOS

Los funcionarios y/o trabajadores de la Universidad son responsables de la información que manejan y deberán seguir los siguientes lineamientos para protegerla y evitar pérdidas, accesos no autorizados y utilización indebida de la misma.

5.3.1. Almacenamiento de la Información

a. Toda información crítica debe estar encriptada, ya sea que se encuentre al interior de la Institución o externamente, en cualquier medio de almacenamiento, transporte o transmisión.

b. Toda información sensible debe tener un proceso periódico de respaldo, tener asignado un período de retención determinado, la fecha de la última modificación.

c. Garantizar que todas las copias de resguardo de información y software sean documentadas correctamente, y que sean probadas con regularidad para garantizar que se puede contar con ellas en caso de emergencia.

d. Preparar la creación oportuna de copias de resguardo de toda la información y software que se requiera para respaldar las actividades esenciales y los planes de contingencia.

e. Enviar la información de resguardo con prontitud y de forma segura a un lugar de almacenamiento remoto seguro. Este lugar debe estar lo suficientemente apartado de las instalaciones primarias para que la posibilidad de que ambos se vean afectados por el mismo incidente al mismo tiempo sea remota.

f. Retener suficiente información de resguardo generada para los requerimientos básicos, legales y regulatorios.

5.3.2. Administración de la Información

a. Cualquier tipo de información interna de la entidad no debe ser vendida, transferida o intercambiada con terceros para ningún propósito diferente para la que fue elaborada, y se debe cumplir con los procedimientos de autorización internos para los casos en que se requiera.

b. Todos los derechos de propiedad intelectual de los productos desarrollados o modificados por los empleados de la Institución,

durante el tiempo que dure su relación laboral, son de propiedad exclusiva de la Institución.

c. Los datos y programas de la Institución deben ser modificados únicamente por personal autorizado de acuerdo con los procedimientos establecidos, al igual que el acceso al Centro de Datos debe restringirse únicamente al personal autorizado.

d. Cuando la información sensible no se está utilizando se debe guardar en los sitios destinados para eso, los cuales deben contar con las debidas medidas de seguridad que garanticen su confidencialidad e integridad.

e. En cualquier momento, el propietario de la información con la participación del responsable de la Unidad de Informática puede reclasificar el nivel de sensibilidad inicialmente aplicado a la información.

f. Todo software que comprometa la seguridad del sistema se custodiará y administrará únicamente por personal autorizado.

g. La información de la Institución no debe ser divulgada sin contar con los permisos correspondientes, además, ningún empleado, contratista o consultor debe tomarla cuando se retire de la Institución.

h. Todos los medios de almacenamiento utilizados en el proceso de construcción, asignación, distribución o encriptación se deben someter a un proceso de eliminación inmediatamente después de ser usados.

i. Toda la información histórica almacenada debe contar con los medios, procesos y programas capaces de manipularla sin inconvenientes, esto teniendo en cuenta la reestructuración que sufren las aplicaciones y los datos a través del tiempo.

5.4. HARDWARE

La administración, mantenimiento, modernización y adquisición de equipos computacionales y de telecomunicaciones deben adoptar los siguientes lineamientos para proteger la integridad técnica de la Institución.

5.4.1. Cambios al Hardware

a. Los equipos computacionales de la Institución no deben ser alterados ni mejorados (cambios de procesador, memoria, tarjetas u otros) sin la evaluación técnica y autorización de la Unidad de Informática.

b. Los funcionarios y/o trabajadores deben reportar al área pertinente de la Institución sobre daños y/o pérdida del equipo que tengan a su cargo y sea propiedad de la Institución. La intervención directa para reparar el equipo está prohibida. La Institución debe proporcionar personal interno o externo para la solución del problema reportado.

c. Todos los equipos de la entidad deben estar relacionados en un inventario que incluya la información de sus características, configuración y ubicación.

d. Todo el hardware que adquiera la Institución debe realizarse a través de los canales de compra correspondientes.

e. Para todos los equipos y sistemas de comunicación utilizados en la entidad, se debe aplicar un procedimiento formal de control de cambios que garantice que sólo se realicen los cambios autorizados. Este procedimiento de control de cambios debe incluir la documentación del proceso con las respectivas propuestas revisadas, la aprobación de las áreas correspondientes y la manera como el cambio fue realizado.

f. Todos los productos de hardware adquiridos deben contar con el respectivo documento de garantía y/o mantenimiento.

g. Los equipos computacionales, ya sean estas computadoras, servidores, LAN, etc. no deben moverse o reubicarse sin la aprobación previa del área involucrada.

5.4.2. Acceso Físico y Lógico

a. Antes de conectarlos a la red interna todos los servidores de Intranet de la Institución deben ser autorizados por el área responsable del hardware.

b. Las bibliotecas de discos duros y documentos se deben ubicar en áreas restringidas en el DataCenter y en sitios alternos con acceso únicamente a personas autorizadas.

c. Todas las conexiones con los sistemas y redes de la entidad deben ser dirigidas a través de dispositivos probados y aprobados por la organización y contar con mecanismos de autenticación de usuario.

d. Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de La Institución deben ser restringidas.

e. Todas las líneas que permitan el acceso a la red de comunicaciones o sistemas multiusuario deben pasar a través de un punto de control adicional (firewall) antes de que la pantalla de login aparezca en la terminal del usuario.

5.4.3. Respaldo y Continuidad de las Actividades

a. La administración debe proveer, mantener y dar entrenamiento sobre los sistemas de protección necesarios para asegurar la continuidad del servicio en los sistemas de computación críticos, tales como sistemas de detección y eliminación de fuego, sistemas de potencia eléctrica suplementarios y sistemas de aire acondicionado, entre otros.

b. Los equipos del DataCenter se deben equipar con unidades suplementarias de energía eléctrica como el UPS y el Grupo Electrógeno.

c. El diseño de la red de comunicaciones debe estar de tal forma que se evite tener un punto crítico de falla, como un centro único que cause la caída de todos los servicios.

d. Los backups de los sistemas de computación y redes deben ser almacenados en una zona diferente de donde reside la información original.

e. A todo equipo de cómputo, comunicaciones y demás equipos de soporte debe realizársele un mantenimiento preventivo y periódico, de tal forma que el riesgo a fallas se mantenga en una probabilidad de ocurrencia baja.

f. Los planes de contingencia y recuperación de equipos deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe documentarse y sus resultados y las acciones de corrección deben comunicarse a la alta dirección.

5.4.4. Otros

a. Los equipos portátiles de computación que contengan información sensible deben utilizar software de encriptación para proteger la información.

b. Todo equipo de cómputo y de comunicaciones de la Institución debe tener un código de identificación permanente grabado en el equipo, además, los inventarios físicos se deben realizar en forma periódica, regular y eficiente.

c. Todo equipo portátil debe tener una Declaración de Responsabilidad, la cual incluya instrucciones de manejo de información y acato de normas internas y de seguridad para el caso de robo o pérdida.

5.5. INSTALACIONES FISICAS

Todos los funcionarios y/o trabajadores de la Institución deberán seguir los siguientes lineamientos de seguridad física con el fin de salvaguardar los recursos técnicos y humanos de la Institución.

5.5.1. Control de acceso físico

La Institución debe contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control inteligente y sistemas de alarmas en las dependencias que se consideren críticas.

a. Personas

i. Los terceros visitantes al Data Center deben estar acompañados por el personal de la Unidad de Informática, además, deben portar un distintivo visible que los acredite como tal. De igual manera se debe proceder con el personal de la Institución que requiera ingresar al Centro de Datos. Además, tanto los terceros como el personal de la Institución deben tener la información y recursos necesarios para el desarrollo de sus actividades.

ii. En el evento que los funcionarios y/o trabajadores dejen de tener vínculos laborales con la entidad todos sus códigos de acceso deben ser cambiados o desactivados. Además, en caso de pérdida de la tarjeta de acceso también deben desactivarse dichos códigos.

iii. Se debe mantener el registro de acceso del personal autorizado y de ingresos con el objeto de facilitar procesos de investigación.

iv. Como mecanismo de prevención todos los empleados y visitantes no deben comer, fumar o beber en el DataCenter o en instalaciones con equipos tecnológicos. Al hacerlo estarían exponiendo los equipos a daños eléctricos como a riesgos de contaminación sobre los dispositivos de almacenamiento.

b. Equipos y otros recursos

i. Toda sede y equipo informático, ya sean propios o de terceros, que procesen información para la Institución o posean un vínculo especial con la misma, debe cumplir con todas las normas de seguridad física que se emitan, con el fin de evitar el acceso a personas no autorizadas a las áreas restringidas donde se procese o mantenga información secreta, confidencial y privada, y asegurar la protección de los recursos de la plataforma tecnológica y su información.

ii. Los equipos computacionales no deben moverse o reubicarse sin la autorización previa de la Unidad de Informática.

iii. Todos los equipos de propiedad de la Institución no deben retirarse de las instalaciones físicas por ningún personal, a menos que esté previamente autorizado.

iv. No se debe proveer información sobre la ubicación del DataCenter o de los lugares críticos, como mecanismo de seguridad.

5.5.2. Protección física de la información

a. Al terminar la jornada laboral, los escritorios y áreas de trabajo deben quedar desprovistos de documentos sensibles que puedan comprometer los intereses de la Institución. Estos deben quedar bajo llave en archivadores, cajas fuertes o demás medios de almacenamiento físico seguros.

b. Las áreas donde se maneja información crítica deben contar con cámaras que registren las actividades realizadas por los funcionarios y/o trabajadores.

5.5.3. Protección contra desastres

Dado que cualquier tipo de desastre natural o accidental ocasionado por el hombre puede afectar el nivel de servicio y la imagen de la Institución, se deba prever que los equipos de procesamiento y

comunicaciones se encuentren localizados en áreas aseguradas y debidamente protegidas contra inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con el buen uso de los equipos y la continuidad del servicio.

5.5.4. Planes de emergencia, contingencia y recuperación

a. Es responsabilidad de la Dirección General de Administración el preparar, actualizar y probar los planes de Contingencias, Emergencias y Recuperación previendo la continuidad de los procesos críticos para el negocio en el evento de presentarse una interrupción o degradación del servicio.

b. La Unidad de Informática debe establecer, mantener y probar periódicamente el sistema de comunicación que permita a los usuarios de la plataforma tecnológica notificar posibles intromisiones a los sistemas de seguridad, estos incluyen posibles infecciones por virus, intromisión de hackers, divulgación de información no autorizada y debilidades del sistema de seguridad.

c. El Plan de Contingencia y de Recuperación debe permanecer documentado y actualizado de manera tal que sea de conocimiento general y fácilmente aplicable en el evento de la presencia de un desastre, permitiendo que los recursos previstos se encuentren disponibles y aseguren la continuidad de los procesos de negocio, en un tiempo razonable para cada caso y contemplando como mínimo los riesgos más probables de ocurrencia que afecten su continuidad.

d. El mantenimiento del plan de Contingencias y Recuperación general debe incluir entre otros un proceso estándar que integre los planes de contingencia para computadores y comunicaciones, así como también el inventario de hardware, software existente y los procesos que correrán manualmente por un período de tiempo.