INABVE
PAZ, RECONCILIACIÓN, REINSERCIÓN

GOBIERNO DE EL SALVADOR

VERSIÓN PÚBLICA

"Este documento es versión pública, por lo que, únicamente se ha omitido la información que la Ley de Acceso a la Información Pública (LAIP) define como confidencial, por su carácter privado tales como datos personales de las personas naturales firmantes". (Artículo 24 y 30 de la LAIP para la publicación de la información oficiosa)

POLÍTICAS DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Sello	Sello	Sello	Acuerdo: 19.9 Acta: CXXXIV 25/11/2022
Jefe de TICS	Director de Planificación	Dr. Daniel Platero Gerente General	Junta Directiva
Elaboró	Revisó	Visto Bueno	Aprobó

PROPÓSITO

Las Tecnologías de la Información y comunicación (TIC) son el conjunto de herramientas, recursos y programas que se utilizan para el procesamiento, intercambio, almacenamiento de datos y administración de información, mediante diversos soportes tecnológicos.

Su finalidad es garantizar la emisión, acceso y tratamiento de la información, a través de distintos códigos que puedan corresponder a textos, vídeos, imágenes y sonidos, por lo tanto, las TIC se han convertido en recursos fundamentales para garantizar la ejecución de los procedimientos administrativos de la institución puesto que permiten agilizar el flujo de información y aumentar el alcance de los receptores.

Por esta razón, es necesario establecer lineamientos que regulen el acceso a las TIC, su control, resguardo y las responsabilidades de administración por parte de la Unidad de Tecnologías de la Información y Comunicaciones y los usuarios internos de estos recursos.

COMPROMISOS

- Gestionar con proveedores la adquisición de los equipos de información y comunicación de la institución.
- Dar seguimiento a las solicitudes de hardware, software y creación de usuarios de las diferentes áreas organizativas del INABVE.
- Asegurar el funcionamiento continuo de los equipos de información y comunicación mediante los mantenimientos preventivos, correctivos y soporte técnico al personal.
- Establecer las responsabilidades de los usuarios para el correcto uso y resguardo de los equipos del instituto y para el personal de la Unidad de Tecnologías de la Información y Comunicación en la creación de usuarios y manipulación de los equipos.

OBJETIVO

Regular los aspectos comunes a los diferentes servicios y actividades informáticas utilizadas dentro del INABVE, garantizando el acceso y resguardo de la información digital de las diferentes áreas organizativas a través del uso adecuado del Software y Hardware y, el buen uso de los recursos de la Unidad de Tecnologías de la Información y Comunicaciones conforme a los valores institucionales.

DE LA GESTIÓN Y ADMINISTRACION DE CONTRASEÑAS

I. CREACIÓN DE CONTRASEÑAS

1. Todas las contraseñas de nivel de usuario y de sistema deben ajustarse a estas políticas de creación contraseñas.
2. Los usuarios no deben usar la misma contraseña para acceso a cuentas de la empresa que utilice para otro tipo de accesos no relacionados (por ejemplo, cuentas de correo personal, redes sociales, etc.).
3. Los usuarios no deben usar la misma contraseña para diferentes necesidades de acceso de la empresa.
4. Debe tener como mínimo 8 caracteres.
5. Debe tener como mínimo un número, una letra minúscula y una letra mayúscula.
6. Debe tener al menos un carácter especial.
7. Deben tener un periodo de caducidad.
8. Todas las contraseñas de nivel de sistema (por ejemplo, usuario root, admin, administrador, cuentas de administrador de aplicaciones, etc.) debe de ser cambiadas al menos cada seis meses.
9. Todas las contraseñas de nivel de usuario (por ejemplo: de correo electrónico, navegación web, computadoras de escritorio, etc.) deben cambiarse al menos cada tres meses.
10. Corresponderá a TICS definir los diferentes niveles de accesos o permisos jerárquicos de los sistemas a asignar por usuario de todas y cada una de las áreas, para poder de esa forma controlar el acceso a los logueos e información ingresada a los sistemas.
11. Es responsabilidad de cada usuario personalizar las contraseñas de carácter temporal y mantener la confidencialidad de estos datos.

II. RESTABLECIMIENTO DE CONTRASEÑAS

1. Para realizar un reseteo el personal de infraestructura y/o seguridad informática creara una contraseña genérica y se deberá solicitar que el usuario ingrese una nueva cumpliendo con todo el apartado.
2. Si se detecta que el usuario solicita un mínimo de 5 veces el reseteo de contraseña en un mes se le indicara por medio de correo a su superior, por mala gestión de sus credenciales.

III. PROTECCIÓN DE CONTRASEÑAS

1. Las contraseñas no deben de compartirse con nadie. Todas las contraseñas deben ser tratadas como sensibles, como información confidencial de la empresa.
2. Las contraseñas que no sean genéricas, no se deben adjuntar en mensajes de correo electrónico u otras formas de comunicación electrónica.
3. Las contraseñas no deben ser reveladas por teléfono a nadie.

4. No debe de revelar contraseñas en cuestionarios o formularios de seguridad o de ningún tipo.
5. La contraseña no debe incluir nombres o números relacionados al usuario ni a la unidad a la que pertenece.
6. El acceso se bloqueará después de repetir 5 veces las credenciales de forma errónea.
7. No se podrá reutilizar la misma contraseña.
8. No deje pistas del formato de una contraseña (por ejemplo, "Apellido de mi familia").
9. No comparta contraseñas de la empresa con nadie, incluyendo asistentes, administrativos, secretarias, directivos, dueños, socios, compañeros de trabajo durante las vacaciones, amigos o miembros de la familia.

IV. ADMINISTRACIÓN ADECUADA DE CONTRASEÑAS PARA LOS USUARIOS

1. No escriba ni guarde contraseñas en notas adhesivas o papel en cualquier lugar de su oficina. (Por ejemplo, paredes, escritorios, sillas, cubículos, monitores o en el case de las computadoras, etc.)
2. No guarde las contraseñas en archivos en su computadora o dispositivos móviles (teléfonos, tablets) sin cifrado.
3. No utilice la función "Recordar Contraseña" de aplicaciones (por ejemplo, navegadores web)
4. Se recomienda utilizar un sistema gestor de contraseñas (Por ejemplo, Dashlane, LastPass, Bitwarden) o memorizar las contraseñas.
5. Cualquier usuario que sospeche que su contraseña puede haber sido comprometida debe reportar el incidente inmediatamente y cambiar todas sus contraseñas a la brevedad.

V. ADMINISTRACIÓN DE ACTIVE DIRECTORY

1. Se deben usar cuentas con permiso de administración al AD y no la propia cuenta de administrador del servidor.
2. Se debe acceder al AD por medio de una red especifica indicada por el personal de infraestructura y no desde cualquier red de la institución.
3. Se debe utilizar una nomenclatura homogénea para nombrar, unidades organizativas, grupos, usuarios, objetos, etc.
4. Cada usuario, grupo y objeto del AD debe estar ubicado en la unidad organizativa a la que pertenece.

VI. CREACIÓN DE USUARIOS EN ACTIVE DIRECTORY

1. La nomenclatura para la creación de usuarios deberá ser utilizando el nombre completo del usuario con la primera letra mayúscula en cada nombre y apellido.
2. Para la creación de las credenciales de acceso a la cuenta del AD la nomenclatura deberá ser utilizando el primer nombre y apellido del usuario separados por un

punto, agregando al final el nombre del dominio de la institución. En caso de que el primer nombre y apellido se repitan con el de otro usuario ya existente, se deberá agregar después del primer nombre la primera letra de su segundo nombre y seguir con la nomenclatura especificada.

VII. CREACIÓN DE GRUPOS EN ACTIVE DIRECTORY

1. La nomenclatura para la creación de grupos deberá ser utilizando la palabra "Usuarios" seguido de un guion bajo y el acrónimo de la gerencia, dirección, unidad o departamento en el que se creará el grupo.
2. Los usuarios que pertenecerán a cada grupo deben estar especificados por el responsable de cada gerencia, dirección, unidad o departamento.

VIII. CREACIÓN DE UNIDADES ORGANIZATIVAS EN ACTIVE DIRECTORY

1. La nomenclatura para la creación de unidades organizativas deberá ser utilizando el nombre en mayúsculas separando con un guion bajo cada palabra que tenga la gerencia o dirección que se creará.
2. La nomenclatura para la creación de unidades organizativas que están bajo otra unidad organizativa que sea gerencia o dirección deberá ser utilizando el acrónimo en mayúsculas del departamento o unidad que se cree.

IX. RESETEO DE CONTRASEÑAS

1. El reseteo de contraseñas deben realizarla únicamente los administradores del AD o delegados por el administrador en el caso que sea de una regional especifica.
2. Se debe seguir el apartado de gestión de contraseñas para realizar la gestión.

X. INGRESO DE EQUIPOS Y OBJETOS AL AD

1. Las computadoras que se ingresen en el domino de la institución deben ser ingresados con la siguiente nomenclatura:

   Indicar si es un equipo portátil o de escritorio con las letras en mayúsculas "PT" o "PC" seguido del número correlativo asignado por el personal de soporte técnico, continuando con el acrónimo en mayúsculas de la gerencia, dirección, unidad o departamento al que va a pertenecer el equipo esto seguido de un guion medio para finalizar con la letra en mayúscula del área física (C= área central, N= área norte, S= área Sur, O= área oeste) y el número del nivel de planta (1, 2, 3 o 4).

2. Las impresoras que se ingresen en el dominio de la institución deben ser ingresadas con la siguiente nomenclatura:

   El nombre que se asignara empezara por las letras "IM" seguido del correlativo asignado por el personal de soporte técnico, continuando con el acrónimo en mayúsculas de la gerencia, dirección, unidad o departamento al que va a pertenecer.

la impresora esto seguido de un guion medio para finalizar con la letra en mayúscula del área física (C= área central, N= área norte, S= área Sur, O= área oeste) y el número del nivel de planta (1, 2, 3 o 4).

En caso de que la impresora se ingrese en calidad de préstamo se le asignaran las letras "IMP" seguido de la nomenclatura mencionada en el apartado anterior.

3. Los servidores que se ingresen en el dominio de la institución deben ser ingresadas con la siguiente nomenclatura:

   Sí es un servidor físico el nombre que se asignara empezará por las letras "SV" seguido de dos números que indiquen el correlativo, esto será asignado por el área de infraestructura, continuando con el acrónimo en mayúsculas de la unidad de informática, esto seguido de un guion medio para finalizar con la letra en mayúscula del área física (C= área central, N= área norte, S= área Sur, O= área oeste) y el número del nivel de planta (1, 2, 3 o 4).

   Sí es un servidor virtual el nombre que se asignara empezara por las letras "VM" seguido de dos números que indiquen el correlativo, esto será asignado por el área de infraestructura continuando con máximo 6 letras mayúsculas que indiquen el tipo de servicio que están ejecutando esto seguido de un guion medio para finalizar con la letra en mayúscula del área física (C= área central, N= área norte, S= área Sur, O= área oeste) y el número del nivel de planta (1, 2, 3 o 4).

XI. ADMINISTRACIÓN DE OFFICE365 ®

1. Se debe utilizar una nomenclatura homogénea para nombrar a los usuarios de correo.
2. Cada usuario debe tener especificado el cargo que desempeñará en la institución y la unidad a la que ingresará, esto deberá ser proporcionado por el área de RRHH. En caso no se proporcione se deberá notificar por correo electrónico que no se tiene la información completa.

XII. CREACIÓN DE USUARIOS OFFICE365 ®

1. La nomenclatura para la creación de usuarios deberá ser utilizando el nombre completo del usuario con la primera letra mayúscula en cada nombre y apellido.
2. Para la creación de las credenciales de acceso a la cuenta de Office la nomenclatura deberá ser utilizando el primer nombre y apellido del usuario separados por un punto, agregando al final el nombre del dominio de la institución.
   En caso de que el primer nombre y apellido se repitan con el de otro usuario ya existente, se deberá agregar después del primer nombre la primera letra de su segundo nombre y seguir con la nomenclatura especificada.
3. Para la creación de cuentas grupales la nomenclatura deberá ser utilizando el nombre de la gerencia, dirección, unidad o departamento que lo solicita, separando

cada palabra por un punto agregando al final el nombre del dominio de la institución. En caso se requieran múltiples cuentas grupales de la misma gerencia, dirección, unidad o departamento que lo solicitase asignara un numero siguiendo el orden correlativo.

XIII. ASIGNACIÓN DE LICENCIAS DE OFFICE365 ®

1. Las licencias básicas deberán ser asignadas a usuarios que únicamente necesitan correo electrónico.
2. Las licencias estándar se asignarán a cuentas grupales y usuarios que necesiten todas las herramientas de ofimática, este tipo de licencia deberá ser solicitada por el encargado de la gerencia, dirección, unidad o departamento al que pertenece el usuario justificando la necesidad de este tipo de licencia.

XIV. ADMINISTRACIÓN DE FIREWALL

1. Se debe acceder al firewall por medio de una red especifica indicada por el personal de infraestructura informática y no desde cualquier red de la institución.
2. Se deben tener agregados por medio de dirección IP o dirección MAC los activos de la red como Servidores, APs, Cámaras, Impresoras, Marcadores.
3. La nomenclatura para agregar nombres a equipos de red como Switches o APs deberá ser utilizando las letras "SW" o "AP" seguido de dos números que indiquen el correlativo, esto será asignado por el personal de infraestructura informática continuando con máximo 4 letras mayúsculas que indiquen la gerencia, dirección, unidad o departamento donde se encuentran esto seguido de un guion medio para finalizar con la letra en mayúscula del área física (C= área central, N= área norte, S= área Sur, O= área oeste) y el número del nivel de planta (1, 2, 3 o 4).
4. Si se necesitan políticas específicas de red para una gerencia, dirección, unidad o departamento, la jefatura de dicha área deberá especificar por medio de un correo al jefe de la unidad de TICS cuales son las redes con las que necesitan tener comunicación y porque motivo.

XV. ADMINISTRACIÓN DE PLATAFORMAS ADOBE, AUTODESK Y SKETCHUP

1. Se deberá solicitar y justificar por medio de correo a la jefatura de TICS la asignación de licencias para usuarios específicos de la institución.
2. La creación de usuarios deben realizarla únicamente el personal del área de infraestructura.
3. La nomenclatura para la creación de usuarios deberá ser utilizando el nombre completo del usuario con la primera letra mayúscula en cada nombre y apellido.
4. Para la creación de las credenciales de acceso a las cuentas la nomenclatura deberá ser utilizando el primer nombre y apellido del usuario separados por un punto, agregando al final el nombre del dominio de la institución. En caso de que primer nombre y apellido se repitan con el de otro usuario ya existente, se deberá

agregar después del primer nombre la primera letra de su segundo nombre y seguir con la nomenclatura especificada.

XVI. CREACIÓN DE USUARIOS PARA TARJETAS DE ACCESO

1. La creación de usuarios deben realizarla únicamente el personal del área de infraestructura informática.
2. La nomenclatura para la creación de usuarios deberá ser utilizando el nombre completo del usuario con la primera letra mayúscula en cada nombre y apellido.
3. Para asignar una tarjeta de acceso al personal de la institución, se deberá enviar la solicitud por correo a la jefatura de TICS y seguir el procedimiento administrativo.
4. Para asignar una tarjeta de acceso a personas visitantes se deberá enviar la solicitud y justificar por correo a la jefatura de TICS y seguir el procedimiento administrativo.

XVII. ADMINISTRACIÓN DE ENDPOINT

1. Se debe acceder al Endpoint por medio de una red especifica indicada por el personal de infraestructura informática y no desde cualquier red de la institución.
2. Cada uno de los equipos de la institución debe estar agregado al Endpoint.
3. Para deshabilitar el Endpoint de algún equipo se solicitará y justificará por medio del jefe correspondiente al jefe de la unidad de TICS y el personal de soporte técnico o infraestructura informática deberá realizarlo.
4. Si se necesitan políticas específicas de permisos a sitios web para una gerencia, dirección, unidad o departamento, la jefatura de dicha área deberá especificar por medio de un correo al jefe de la unidad de TICS cuales son los sitios que necesitan y porque motivo.

DEL HARDWARE: EQUIPOS, DISPOSITIVOS, Y APARATOS

I. ADQUISICIÓN, ASIGNACIÓN Y MANTENIMIENTO DE EQUIPOS TECNOLÓGICOS

1. La unidad de TICS será la única responsable de hacer requerimientos de los equipos, dispositivos o aparatos informáticos según las necesidades que se presenten en cada área de trabajo; por lo anterior, deberá participar en los contratos de adquisición de estos bienes o servicios.
2. Para toda solicitud de adquisición de Recursos Tecnológicos, será la Unidad de Tecnologías de la Información y Comunicaciones del INABVE quien proporcione las especificaciones técnicas correspondientes, basadas en el respectivo análisis técnico, económico y funcional con el propósito de seleccionar el producto que mayor beneficio represente para la Institución.
3. La unidad de TICS deberá evaluar que los equipos, dispositivos o aparatos de informática cumplan con las especificaciones indicadas en los requerimientos de compra.

4. Corresponderá a TICS la asignación e instalación de los equipos adquiridos, así como de la disponibilidad de energía eléctrica, cableado estructurado y las condiciones físicas aceptables.
5. Toda planificación para mejora o traslado de las TIC deberá contar con la asesoría y el visto bueno de la Unidad de Tecnologías de la Información y Comunicaciones del INABVE, quien deberá estar informado con anticipación de todo el proceso y deberá de concluirlo o recibirlo para certificar si cumple con lo requerido antes de ser utilizado formalmente.
6. Será responsabilidad de la unidad de TICS evaluar el área física donde se instalarán nuevos equipos informáticos, confirmando que el área cuenta con condiciones óptimas para la instalación de este.
7. La incorporación de nuevos empleados deberá ser informada con 15 días de anticipación y de forma escrita a la Unidad de Tecnologías de la Información y Comunicaciones del INABVE, para que este analice la compra o reasignación del recurso tecnológico más adecuado a utilizar.
8. Para mantener un mayor periodo de garantía, se adquirirá hardware nuevo, no remanufacturado, de una marca que cuente con representación legal en el país y brinde un tiempo de 1 a 3 años de garantía.
9. El mantenimiento preventivo o correctivo de las TIC en la institución es responsabilidad de la Unidad de Tecnologías de la Información y Comunicaciones del INABVE, quien garantizará el correcto funcionamiento de estas.
10. Las labores de mantenimiento deberán ser calendarizadas de forma anual, semestral o trimestral según sea la necesidad en cada caso. Las áreas administrativas deberán respetar las actividades planificadas por este departamento, permitiendo las labores de mantenimiento correspondientes.
11. La unidad de TICS tendrá el deber de vigilar y llevar el control detallado de los equipos, dispositivos o aparatos de hardware del instituto, acorde con las necesidades existentes de la misma.
12. Será responsabilidad de TICS verificar que los equipos adquiridos sean asignados a empleados permanentes y no se podrá asignar a un mismo usuario más de un equipo informático.
13. TICS deberá instruir a los usuarios sobre el uso y manejo adecuado de los equipos, dispositivos y aparatos instalados.
14. La información que circule en cada equipo de TIC será propiedad del INABVE, por lo tanto, debe instarse a los usuarios al uso responsable y eficiente de tal herramienta de trabajo.
15. El INABVE podrá contar con herramientas para el monitoreo del uso de los equipos asignados a cada área organizativa.

II. RESPONSABILIDADES DE LOS USUARIOS

Los usuarios que tengan equipos de TIC asignados en sus áreas de trabajo tendrán las siguientes obligaciones para el manejo apropiado de los equipos:

1. Utilizar los equipos asignados únicamente para ejecutar las actividades o tareas Institucionales.
2. Los usuarios deberán firmar la correspondiente acta de asignación de equipo informático verificando que las especificaciones correspondan a lo entregado.
3. Informar oportunamente el mal funcionamiento o necesidades de reparación de su equipo.
4. No podrán usar equipos tecnológicos personales como: laptops, tablets u otros dispositivos informáticos, en el área de trabajo.
5. No podrá ingresar dispositivos o equipos tecnológicos personales a la institución sin la respectiva autorización.
6. No podrá efectuar solicitudes a la Unidad de TICS, de reparación de equipos tecnológicos personales.
7. Solicitar a la Unidad de TICS los equipos, dispositivos, aparatos y programas informáticos necesarios que requiera el área.
8. Entregar o devolver los equipos en buenas condiciones o con el normal desgaste de uso, en caso de que se le haya sido requerido o a su finalización de contrato.
9. En caso de robo, pérdida o hurto deberá de interponer la denuncia policial y a su vez informar a la Unidad de Tecnologías de la Información y Comunicaciones del INABVE sobre el hecho, para recibir instrucciones.
10. El usuario deberá responder por los costos incurridos en caso de daño por negligencia o descuido del equipo de TIC asignado.
11. Los jefes de cada unidad, dirección o gerencia deberán informar y solicitar a la Unidad de TICS la autorización de poder sacar el equipo institucional asignado para laborar fuera de las oficinas o del horario de trabajo.

iii. ADMINISTRACIÓN DE CÁMARAS

1. Únicamente tendrán acceso inmediato al sistema de cámaras: Jefe de TICS, Presidente del INABVE, Gerente General, Jefe de Seguridad y personal que el asigne para el monitoreo.
2. Nadie externo a la institución puede tener, ni debe pedir acceso, al sistema de cámaras.
3. Si algún empleado de la institución por A o B razón necesita el acceso al sistema de cámaras y grabaciones de seguridad lo deberá solicitar por medio de correo o memorando, con apoyo de su jefatura inmediata, a la jefatura de TICS. Deberá explicar el motivo de uso además de la fecha y hora especificas a revisar.

DEL SOFTWARE, LICENCIAS Y PROGRAMAS DE COMPUTADORAS

I. LICENCIAS Y PROGRAMAS INFORMÁTICOS

1. Será responsabilidad de TICS custodiar, almacenar y llevar el control del inventario de software (licencias y programas) instalados en los equipos informáticos del INABVE, así como verificar que todo el software instalado en él este legalmente licenciado.
2. Para mantener la legalidad de las licencias se adquirirán equipos con el licenciamiento que da el fabricante para las instituciones de gobierno, cuando aplique.
3. Los programas informáticos instalados en la Institución estarán amparados con las respectivas licencias extendidas por el fabricante, otorgando al INABVE el derecho de instalación y uso de estos.
4. Establecer configuraciones automatizadas para que los usuarios guarden toda su información en dichos sistemas y puedan resguardar la información facilitando las copias de seguridad.

II. RESTRICCIONES Y DEBERES DE LOS USUARIOS

1. Está prohibido instalar y/o descargar juegos, videos, música y aplicaciones de cualquier tipo que no guarden relación con el desarrollo de labores diarias del Instituto.
2. Está prohibido tener y conectar a los equipos dispositivos de almacenamiento que no sean los asignados por la Unidad de TICS o no guarden relación con la institución.
3. Informar inmediatamente a la Unidad de TICS al observar comportamiento inadecuado o sospechoso en los sistemas.
4. Está prohibido tener en los dispositivos de almacenamiento, archivos que no tengan o guarden relación con el INABVE. Tales como:
    a. MP3 (u otro formato de música)
    b. EXE (archivos ejecutables)
    c. MSI (archivos de instalación)
    d. JPG; JPEG, GIF, BMP, PNG, ETC (imágenes)
    e. INI (Archivos de configuración de instalación)
    f. INF (Archivos de configuración de instalación)
    g. DLL (librerías de archivos)
    h. ZIP (archivos comprimidos, por lo regular son archivos personales y aplicaciones)
    i. RAR (archivos comprimidos, por lo regular son archivos personales y aplicaciones)
    j. Entre otros
5. Está prohibido desinstalar el Antivirus del equipo asignado, ya que es de alto riesgo para la seguridad ante el peligro de los virus.

6. Deberá informar a la Unidad de TICS, en caso de presentarse cualquier problema de virus en el equipo asignado.

III. SEGURIDAD INFORMÁTICA

1. Todos los sistemas de informática deberán estar resguardados dentro del área asignada a la Unidad de TICS.
2. Los Usuarios o visitantes externos no podrán acceder al área destinada a la Unidad de TICS, sin la previa autorización del jefe o acompañados de un técnico de la Unidad.
3. Solo podrán acceder al área de infraestructura informática el jefe o/y los técnicos de la Unidad de TICS.
4. Solamente el personal del INABVE será usuario del Sistema Informático de la institución.
5. El acceso a la información institucional está restringido para las personas que no tienen la debida autorización, ya sea en el uso de la computadora, la comunicación entre datos de la red y los sistemas de aplicación institucionales.
6. La información de los sistemas transaccionales se almacena en diferentes servidores para evitar centralización de Bases de Datos.
7. La administración, configuración e implementación de todos los servidores, equipos de red, servicios y plataformas que tenga que ver con la infraestructura tecnológica de la institución deberá ser única mente realizada y gestionada por el personal de esta área.
8. El acceso al área física a los servidores será en horario laboral para el personal autorizado de TICS, fuera de este horario se deberá obtener autorización por parte la jefatura la Unidad de TICS el cual puede ser otorgado o definido personalmente y con anticipación.
9. En caso de acceso al área de servidores por emergencia siempre se deberá notificar de inmediato a la jefatura de la Unidas de TICS.
10. La seguridad de acceso a los recursos de Hardware y Software comprenderá tres niveles:
    a. Nivel 1: la computadora;
    b. Nivel 2: la red; y,
    c. Nivel 3: las aplicaciones institucionales.

    Para cada nivel de seguridad se establecen políticas de acceso tales como: acceso a la red por horarios, cambios de contraseñas de seguridad, suspensiones de accesos cuando el personal deja de trabajar en la institución y otros, por lo que estas actividades se desarrollan en coordinación con los responsables de las diferentes unidades organizativas del INABVE.
11. Se permitirá la utilización de dispositivos ajenos a la institución únicamente con previa autorización de la jefatura de TICS al usuario especifico y previo registro de ingreso.

12. El personal técnico externo podrá entrar a las instalaciones donde se almacena la información confidencial, solamente bajo la vigilancia de personal institucional autorizado y para realizar actividades propias del servicio contratado.
13. El acceso a internet se restringe exclusivamente a través de mecanismos establecidos de seguridad como los cortafuegos incorporados en la red de datos o por servicios de programas Antivirus. No está permitido acceder a Internet por otros medios no autorizados como los módems externos.
14. Cada dispositivo de red inalámbrica (Wifi) se protegerá con una contraseña para que su uso sea controlado, ya sea para acceder a internet o para conectarse a la red de datos institucional.
15. Los datos institucionales en los Sistemas de Información son operativizados a través de un sistema administrador de Base de Datos, el cual contará con mecanismos de seguridad para controlar el acceso de los usuarios de acuerdo con sus roles de trabajo establecidos por la Unidad de TICS, a solicitud del responsable de la unidad de gestión solicitante, para garantizar la integridad, seguridad y recuperación oportuna de la información.
16. Las contraseñas deben establecerse con base en convenciones de seguridad que se detallan en el apartado de gestión de contraseñas,
17. Está prohibido conocer la contraseña de administración, para los usuarios que no sean Administrador de sistemas o ajenos al área de TICS.
18. El acceso a los Sistemas de Información contará con los privilegios o niveles de seguridad para garantizar la protección de la información institucional.
19. Las credenciales para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas y del Servidor.
20. La documentación derivada del desarrollo de sistemas informáticos deberá especificar información sobre el funcionamiento del sistema, tales como: procedimientos claros para el uso, registro, resguardo y recuperación de datos del sistema, lo mismo que los estudios, diagramas y demás escritos realizados para la comprensión del sistema.

DE LO NO CONTEMPLADO

1. Cualquier caso o situación que este fuera de lo contemplado dentro de esta Política será dirimido por Junta Directiva.

GARANTÍA DE DIVULGACIÓN

La presente Política junto con sus objetivos debe ser conocida por los empleados involucrados en los procesos internos de la Unidad de Tecnologías de la Información Comunicaciones del INABVE después de la aprobación de ésta por Junta Directiva.