



MANUAL DE SEGURIDAD Y POLITICAS DE TECNOLOGIA DE LA INFORMACION Y COMUNICACION (TIC)

28 NOVIEMBRE 2019

Instituto Nacional de la Vivienda (INVI)
Creado por: Direccion de Tecnologia (TIC)




“Año del Fomento de las Exportaciones”

28 de Noviembre, 2019

DTI-0910-2019

Al


: **Ing. Mayobanex Escoto**
Director General



Asunto

: **Aprobación de Manual de Seguridad y Políticas de la Dirección TIC, basado en la Norma ISO 27000**

Adjunto

: **Manual de Seguridad y Políticas de la Dirección TIC**

Muy cortésmente, me dirijo a usted con la finalidad de solicitar la aprobación del manual de seguridad y políticas de la Dirección de Tecnología de la Información y Comunicación, basado en el estándar internacional ISO 27000, para fines de seguridad y mantenimiento de políticas y procesos aplicados en esta Institución.

Sin nada más por el momento, se despide,



Ing. Juan Hernández
Director de Tecnología de la Información y Comunicación TIC



JH/mr.



INTRODUCCIÓN:

El manual de políticas y seguridad de Tecnología de la Información y comunicación del Instituto Nacional De La Vivienda (INVI), representa uno de los pilares esenciales en la conservación de la Data, garantizando el buen funcionamiento de los procesos, la integridad de los equipos manejados, la eficiencia en la asistencia brindada al usuario, optimizando los sistemas de calidad de la gestión, así como la evaluación y mejora continua en cada uno de los riesgos establecidos.

La Dirección de Tecnología de la Información y comunicación (TIC), se enfoca en los niveles de seguridad según las normas establecidas a través de los procedimientos marcados con las políticas del área, cada uno de los procedimientos buscan establecer los pasos a seguir para cada uno de los casos a resolver.

Con este manual, se pretende trazar cada uno de lineamientos manejados por esta Dirección, presentando a toda la Institución los procesos y procedimientos en que se maneja el área, para mejoría y claridad en cada uno de ellos, dando a entender el porqué de las acciones tomadas para cada caso, así como el buen uso por parte de los usuarios que conforman este sistema.

Para la elaboración de este manual ha sido preciso la colaboración de todas las áreas de la institución, el método de seguridad en equipos para fines de salvaguardar data, no es posible realizarlo sin la participación de cada uno de los interventores sin distinción de jerarquía, pues todos los usuarios que manejan equipos de TIC, dígase (PC, Teléfonos, etc. En consideración hasta los visitantes en cuanto a monitoreo de cámaras de seguridad,), por eso la colaboración de los funcionarios, usuarios, visitantes están involucrados.

ASPECTOS GENERALES:

El Instituto Nacional de la Vivienda es la Institución rectora y reguladora del sector vivienda del Estado Dominicano. El Instituto Nacional de la Vivienda (**INVI**) fue creado mediante la Ley No. 5892 por el Consejo de Estado el 10 mayo de 1962, con carácter autónomo, sujeto a las prescripciones de esta Ley y a las de los reglamentos que dicta el Poder Ejecutivo como un medio de contribuir a la solución del déficit habitacional existente en el país a través de la construcción de viviendas de interés social.

Misión

Formular, diseñar y ejecutar proyectos habitacionales, integrando a todos los sectores, tanto público como privado en la producción de viviendas para cumplir con el logro de los objetivos del Estado Dominicano referente a la política de vivienda, para beneficiar con un techo seguro a cada familia que no posea vivienda propia, cumpliendo así su rol social. La Misión del **INVI** se basa en satisfacer las necesidades habitacionales de las familias dominicanas de ingresos bajos y medio-bajos con la construcción, Mejoramiento y/o Reconstrucción de viviendas y el otorgamiento de subsidio a través de un **Bono para Vivienda o Bono Tierra**.

Visión

Ser la Institución rectora del Sector Vivienda en el cumplimiento de la política habitacional implementada por el Estado Dominicano, en su objetivo de disminuir el déficit habitacional cuantitativo y cualitativo, fundamentados en nuestra vocación de servicio para cubrir las necesidades de las familias más necesitadas integrando todos los sectores.

Valores

Propiciar un mejoramiento en los niveles y calidad de vida para las familias de bajo y medianos ingresos con la construcción de proyectos habitacionales de bajo costo.

Funciones

- Formular la política, planes y programas nacionales para el Sector Vivienda en conjunto con la Oficina Nacional de Planificación (ONAPLAN).
- Tener a su cargo la producción de viviendas del Sector Público destinadas a familias pertenecientes a grupos de menores ingresos.
- Promover y fomentar la contribución del Sector Privado a la producción de viviendas de bajo costo.
- Dar asistencia técnica y orientar a personas o grupos de personas interesadas en resolver sus necesidades habitacionales, en especial a los grupos organizados.

- Promover el desarrollo de programas urbanos y rurales tomando en cuenta el esfuerzo propio y ayuda mutua.
- Señalar al Poder Ejecutivo la necesidad de expropiación para obtener los terrenos destinados al desarrollo de los programas contenidos en los planes nacionales de vivienda.

Objetivos

- Formular el Plan General de viviendas a nivel Urbano y Rural.
- Ejecutar dicho Plan dentro del marco de sus actividades.
- Promover la contribución privada al desarrollo de dicho Plan.
- Orientar, asesorar y ayudar técnicamente a toda persona o grupo de personas, principalmente las constituidas en cooperativas, de hecho o de derecho que así lo soliciten y dentro de las posibilidades económicas del Instituto.
- Promover el desarrollo de programas Rurales y Urbanos mediante la colaboración de los futuros beneficiarios, siguiendo los principios de esfuerzo propio y ayuda mutua.
- Dirigir sus acciones prioritariamente hacia las familias de ingresos bajos y mínimos, estableciendo programas que apoyen la solución habitacional de dichas familias.

Reglamentaciones

Se definen como:

Mejoramiento y/o Reconstrucción de Vivienda Urbano y Rural en asentamientos humanos con condiciones precarias con participación comunitaria y Mejoramiento y/o Reconstrucción de Viviendas Individual.

Viviendas Nuevas: incluye Viviendas Nuevas para sectores de ingresos bajo y Viviendas Nuevas para sectores de ingresos medio-bajos.

Proyectos Especiales: incluye Fondo de Subsidio Habitacional en coordinación con el sector privado, que es el denominado Programa de Bono para la Vivienda o Bono Tierra y Viviendas Nuevas de Emergencia para las familias damnificados por fenómenos naturales o incendios.

ACUERDOS FIRMADOS POR EL INVI CON ENTIDADES NACIONALES

EL Instituto Nacional de la Vivienda (INVI), durante el período Enero-Octubre de 2019, suscribió varios acuerdos con instituciones públicas y privadas, con el objetivo común de dotar de una vivienda digna a las familias dominicanas de escasos recursos y en situación de vulnerabilidad, a saber:

NO.	NOMBRE DEL ACUERDO	FECHA DE SUSCRIPCIÓN	CONCEPTO DEL ACUERDO	INVOLUCRADOS
1.	Acuerdo Interinstitucional	29/03/2019	Colaboración mutua para la construcción y reparación de viviendas.	INVI-FUNDACIÓN SUR FUTURO
2.	Acuerdo Interinstitucional	28/05/2019	Colaboración mutua para la construcción y reparación de viviendas.	INVI-FARD
3.	Acuerdo Interinstitucional	05/06/2019	Colaboración mutua para la construcción y reparación de viviendas.	INVI-DNCD
4.	Acuerdo Interinstitucional	06/06/2019	Colaboración mutua para la construcción y reparación de viviendas.	INVI-FONPER
5.	Acuerdo Interinstitucional	25/06/2019	Colaboración mutua para la construcción y reparación de viviendas.	INVI-SENASA

Estos acuerdos han contribuido al fortalecimiento de la capacidad de respuesta del Instituto, frente a las solicitudes de construcción y reparación de viviendas, a través de los aportes de materiales, mano de obra y asesoría técnica, realizadas con las instituciones contratantes.

Objetivo del Manual:

Los Objetivos de este manual son los siguientes:

- Definir las políticas que se ejecutan en esta Dirección.
- Concientizar al usuario sobre las políticas establecidas en esta área.
- Promover las normas y derechos de los usuarios de TIC.
- Establecer los riesgos para cada política.

- Realizar los procedimientos de acuerdo a cada una de las políticas
- Presentar al usuario el porqué de cada política y procedimiento llevado a cabo por la Dirección de TIC.
- Mantener actualizados cada uno de los procesos realizados, con las exigencias de los usuarios siempre y cuando no afecten la seguridad e integridad de la Institución y la Data.
- Promover el buen uso de los equipos, así como los sistemas, materias y activos de esta Dirección.

Alcance:

Este manual aplica para todos los empleados de esta Institución, los cuales forman parte del sistema de seguridad Física, así como las aplicaciones de las políticas de la Dirección de Tecnología de la Información y Comunicación.

Propósito:

Estandarizar los procesos de acuerdo con las políticas establecidas en el área, de acuerdo con cada riesgo definido en ellas, para mejora continua del uso y manejo de la plataforma de TIC, garantizando a cada usuario la calidad y seguridad en cada trabajo realizado por medio de sistemas y equipos de tecnología, donde también se le asegure su integridad física por medio a la vigilancia correspondiente ante cualquier eventualidad, asegurando el cumplimiento de cada una de las áreas.

Autorización:

El manual de seguridad y políticas de la TIC, es aprobado por la máxima autoridad, el Director del Instituto Nacional de la Vivienda, así como la aprobación del Director de Tecnología de la Información y Comunicación.

Edición y Distribución

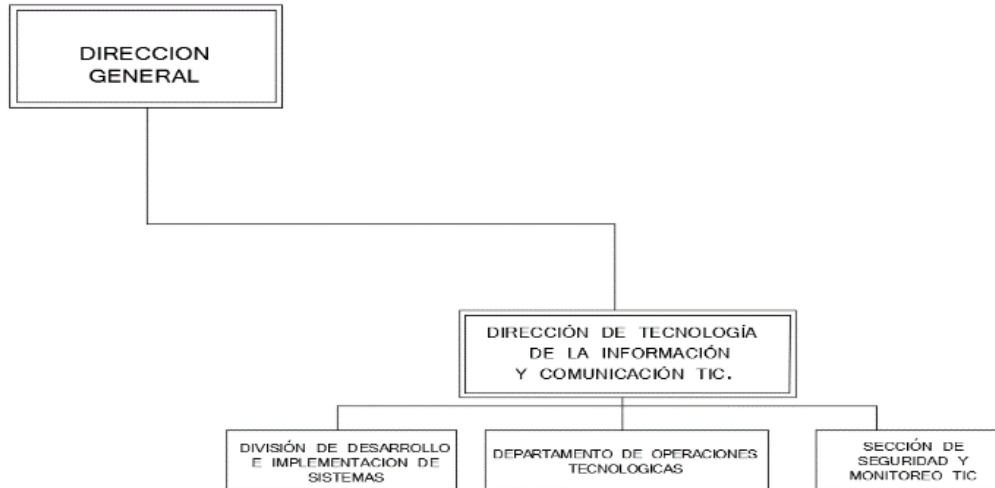
La edición será emitida en formato digital para fines de modificaciones futuras, al igual que la accesibilidad para otras áreas en momento de ser necesitada, la misma no será emitida en formato modificable para dichas áreas.

En formato Físico, será impreso para fines de entrega a la Dirección general, Gerencia de Planificación y Desarrollo y la área ejecutora para fines de respaldo ante cualquier eventualidad o modificación.

Revisiones y Modificaciones:

Ante cualquier modificación será informado el Director de TIC, luego se le emitirá la comunicación y el manual a la Dirección General, Gerencia de Planificación y Desarrollo y las áreas que requieran dicho manual por medio a solicitud.

Organigrama:



Glosario de Términos

A

ACTIVE DIRECTORY

implementación de servicio de directorio en una red distribuida de computadores.. ·

B

BACKUP

Copias o Respaldo de seguridad. ·

BASE DE DATOS

es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. ·

BATCH

se puede definir como la ejecución de un programa sin el control o supervisión directa de usuarios con accesibilidad, o mas bien con los permisos. ·

C

CENTRAL IP

equipo telefónico diseñado para ofrecer servicios de comunicación a través de una base de datos, ubicada por lo general en la sede principal. ·

CLAVE USUARIO

contraseñas para uso personal de cada usuario. ·

COMPUTADORES

Equipo informatico para el procesamiento de datos. ·

CONTROLES DE SEGURIDAD

INFORMATICA

la protección de la infraestructura computacional y todo lo relacionado con esta ·

CORRECTIVO

Que corrige un problema, algo que esta mal. ·

CRM

Gestion de las relaciones con los clientes. ·

D

DATA CENTER

o "centro de datos" en español, es una construcción de gran tamaño donde se albergan los equipos electrónicos necesarios para mantener una red de computadores. ·

DIAGRAMA DE RED

es una forma gráfica de ver las tareas, las dependencias y la ruta crítica del proyecto. ·

DISPONIBILIDAD

Que el acceso este disponible todo el tiempo requerido. ·

DISTRIBUIDOR DE RED

es la disposicion real de los cables de red. ·

F

FORTIGATE

es el único sistema que puede detectar y eliminar virus, gusanos y otras amenazas basadas en contenido, sin afectar al rendimiento de la red, incluso para aplicaciones en tiempo real como la navegación Web. ·

G

GABINETES DE RED

es un gabinete que puede contener dispositivos de red ·

I

INFRAESTRUCTURA DE HARDWARE

El servicio que ofrece el conjunto de dispositivos y aplicaciones necesarios para una empresa. ·

INFRAESTRUCTURA DE SOFTWARE

es la interfaz que interactua con el usuario. diseñada de forma amigable. ·

L

LA CONFIDENCIALIDAD

es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado. ·

LA INTEGRIDAD

se refiere la correctitud y completitud de la informacion en una base de datos.. ·

M

McAfee

Anrivirus. Su utilidad es defender de amenazas de virus, reguardando los datos, manteniendonos seguros de ataques informaticos. ·

N

NVR

graba y administra imágenes ya digitales las cuales son enviadas desde las cámaras IP a través de una red.. ·

P

PLATAFORMA TECNOLOGICA

un gran software que sirve como base para ejecutar determinadas aplicaciones compatibles con este. ·

PREVENTIVO

prevencion de hechos anticipandolos. ·

PROGRAMA INFORMATICO

es una secuencia de instrucciones, escritas para realizar una tarea específica en una computadora. ·

R

RECURSO INFORMATICO

es cualquier componente físico o virtual de disponibilidad limitada dentro de un sistema informático. ·

ROLES ESPECIFICOS

la función o papel que cumple alguien o algo. ·

S

SEGURIDAD DIGITAL

protección de la infraestructura computacional y todo lo relacionado con esta. ·

SEGURIDAD FISICA

refiere a los controles y mecanismos de seguridad dentro y alrededor de la obligación física de los sistemas. ·

SEGURIDAD TIC

la capacidad que tienen las infraestructuras o los sistemas informáticos de disminuir e incluso prevenir los accidentes malintencionados que comprometen la disponibilidad, la autenticidad, la integridad y la confidencialidad de la información. ·

SERVIDORES

es una aplicación en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.. ·

SERVIDORES FISICOS

máquina física integrada en una red informática en la que, además del sistema operativo, funcionan uno o varios servidores basados en software. ·

SERVIDORES VIRTUALES

Son los servidores que toda su funcionalidad está dentro de otro servidor externo. · Véase

SGSI

Sistema de gestión de la seguridad de la información. ·

SISTEMA DE CONTROL DE ACCESO

es un sistema automatizado que permite de forma eficaz, aprobar o negar el paso de personas o grupo de personas a zonas restringidas en función de ciertos parámetros de seguridad establecidos. ·

SISTEMA DE VIGILANCIA

Sistema de video camaras, instaladas por IP. ·

SOFTWARE

La parte lógica de los equipos computacionales, siendo estos programas operadores que funcionan de diferentes formas. ·

STORAGE

La función Data Storage es el conjunto de especificaciones que sirven para definir cómo, cuándo y qué se almacena.. ·

SWITCH

es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local. ·

T

TIC

Tecnologías de la información y comunicación ·

TOPOLOGIA DE RED

mapa físico o lógico de una red para intercambiar datos. ·

W

WINDOWS

Sistema operativo basado en prototipo de ventana, como su nombre en inglés lo indica. ·

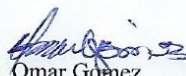
Viernes 15 de Noviembre 2019

DTI-0900-2019

Al : **Ing. Juan Hernández**
Director de Tecnología de la Información y
Comunicación TIC.

Asunto : Solicitud de autorización para implementación
Normas de seguridad Informáticas, ISO 2701.

Cortésmente, me dirijo a usted con la finalidad de solicitar la autorización para el inicio de creaciones e implementaciones de norma ISO 2701 en conjunto con otras normas agregadas a la seguridad Informática, para fines de mejoramiento en el área de seguridad de nuestra institución.


Ing. Omar Gómez
Enc. Infraestructura



JH/mr

Teléfono: 809-732-0600
Fax: 809-227-5803
Correo Electrónico: info@invi.gob.do
Av. Pedro Henriquez Ureña
Esq. Av. Alma Mater, Santo Domingo,
República Dominicana

 [inviRD](#)  [invi_RD](#)  [invi_RD](#)

METODOLOGIA PSI:

En la elaboración de nuestra metodología PSI (Plan de seguridad Informática) destacamos de manera precisa contenido importante para nuestra seguridad, presentando el alcance del SGSI, incluidas las políticas de alto nivel de seguridad, donde se trabajan la matriz de riesgo, realizando la evaluación y tratamiento de los mismos con la finalidad de aplicarlas.

Por medio de la presentación y evaluación de los riesgos es redactado el plan de tratamiento de riesgos, donde se plantean los controles y procedimientos necesarios, luego de esto se procede a implementa programas de capacitación y concienciación acerca de los riesgos para con esto efectuar el tratamiento y plan de mitigación.

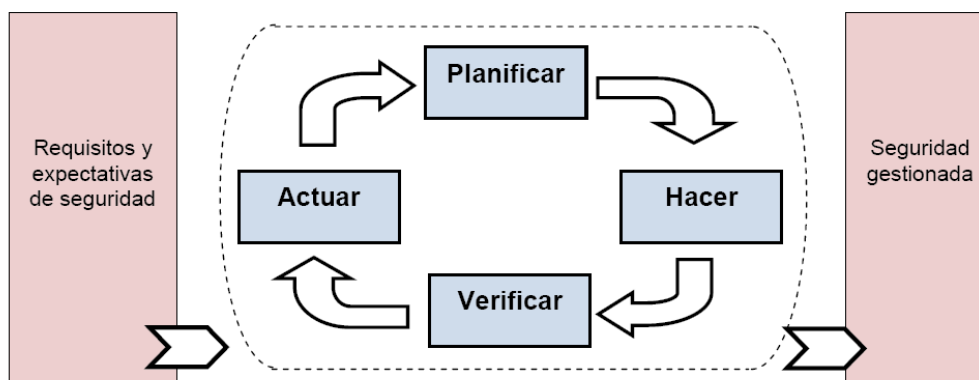
Con la implementación del (SGSI) Sistema de Gestión de la Seguridad de la Información conformamos la estrategia para analizar los aspectos de seguridad, implementando los controles necesarios para garantizar el cumplimiento de lo establecido, con el cual el análisis de riesgo debe contener.

1. Determinar que se trata de proteger
2. Determinar de que es necesario protegerse.
3. Determinar cuan probables son las amenazas.
4. Implementar los controles que protejan los bienes informáticos de una manera rentable.
5. Revisar continuamente este proceso y perfeccionarlo cada vez que una debilidad sea encontrada.

Esta metodología tiene un enfoque basado en procesos con l\el fin de establecer, implementar, operar, dar seguimiento, mantener y mejorar el SGSI de una organización, para ello adopta el modelo de procesos, "Planificar-Hacer-Verificar-Actuar", que se aplica para estructurar todos los procesos del SGSI en correspondencia con la Norma ISO 27001.

Implementación del SGSI

El SGSI se compone de cuatro procesos básicos:



Planificar (Estableciendo el SGSI)

A continuación se desglosan las diferentes políticas establecidas por la dirección de TI, las cuales están relacionadas directamente con el desempeño de las funcionalidades totales del sistema de información manejado.

- Planeación de protocolos.
- Calificar los soportes brindados.
- Asegurar la información manejada por el la institución.
- Identificación de Riesgos.

Hacer (Estableciendo el SGSI)

Tomando en cuenta las diferentes políticas desarrolladas, procedemos a su implementación, contando con todos los requerimientos de lugar para su funcionalidad total. Tomando un enfoque de ejecución y desarrollo, para lograr una funcionalidad completa y desarrollada de las policitas de nuestro sistema de seguridad.

Se realiza cada ejecución de protocolos identificados. Asegurando que todo se haga de la manera correcta, y se ejecuten los procesos adecuadamente.

Se da respuesta inmediata a cada uno de los usuarios, de acuerdo al problema presentado y la dificultad de los mismos, poniendo en espera solo a los problemas de menor importancia, para realizar una solución posterior a ellos.

Mediante un sistema de riesgo, backup, guardado en la nube y servidores virtuales, se resguarda la información procesada por los usuarios, atendiendo a las necesidades actuales del sistema.

Verificar (Estableciendo el SGSI)

La dirección de tecnología, mantiene el control total de los procesos realizados, atendiendo a cada una de las necesidades de los usuarios. Mediante el reporte de los procesos desarrollados, según su solución, se hace una notificación y documentación del cumplimiento del mismo, para evitar en el futuro los mismos problemas previamente identificados, atendiendo así de manera rápida y eficaz al usuario, y al sistema en sí.

Actuar (Estableciendo el SGSI).

Cumpliendo con las normas institucionales, nos aseguramos de ejecutar el plan de acción, revisión y seguimiento de los problemas identificados y solucionados anteriormente. Para lograr un control de los procesos significativamente llevamos a cabo el reporte de cada uno de los procesos realizados por el personal informático, dicho reporte lleva descrito el problema en sí y su solución previa.

El departamento toma en cuenta los trabajos asignados y realizados, tanto que se dan a conocer los detalles de problemas y soluciones para posibles errores futuros.

Al usuario luego de completar con el levantamiento y cumplimiento de las normas para lograr completar la tarea asignada, se le da una breve charla de cómo mejorar su trabajo y como resolver posibles problemas informáticos más adelante, para facilitar los procesos informáticos, y llevar el control del sistema de gestión a su más alta implementación.

Políticas en Área de TIC.

La Dirección de Tecnología de la información, se encarga de resguardar la información de la Institución, velar por el buen uso de los equipos de TIC, mantener el buen estado del hardware y el software manejados por todos los usuarios, a través de mantenimientos, monitores y plan de seguridad informática.

Con la finalidad de una asistencia permanente brindada a los usuarios, la Dirección de Tecnología se compromete con:

- a) Dar asistencia de manera precisa y con los protocolos debidos a cada uno de los usuarios.
- b) Calificar el nivel de soporte brindado dependiendo de las cantidades de soportes en cola.
- c) Asegurar la Data manejada en la institución, así como cada uno del software manejados en cada área.
- d) Identificar riesgos, emitir informes sobre la evaluación de riesgos de acuerdo a cada política.

IMPLEMENTACION DE MEDIDA DE SEGURIDAD.

1. Detectar riesgo y/o recibe reporte de alarma de seguridad y/o situación anómala.
2. Revisar políticas de seguridad activas (Gpo's del Dominio, Firewall, Isa, Proxy, Puertos, Consola Antivirus, seguridad física y lógica, etc.)
3. Revisar nivel de actualización de programas (Sistemas Operativos, aplicaciones, controladores, utilitarios, etc.)
4. Analizar y evalúa efecto de política de seguridad y/o actualización de software.
5. Crear política de seguridad nueva o modificar una existente.
6. Autorizar aplicación seguridad.
7. Probar política de seguridad y/o actualización de software en ambiente de prueba.
8. Implementar política de seguridad y/o actualización de software en ambiente de producción.

Seguridad en los archivos del sistema:

El acceso a los archivos del sistema y al código fuente debe ser restringido. La actualización del software aplicativo y las librerías solo pueden ser llevadas a cabo por los administradores, considerando que para software de proveedores las actualizaciones y migración a nuevas versiones se deben realizar antes de que termine la vigencia del soporte. Los procedimientos de control de cambios deben estar documentados y ser ejecutados bajo los controles adecuados para no comprometer la seguridad de los sistemas.

ACTUALIZACION SOFTWARE DE SISTEMAS (PLATAFORMA Y OTROS)

1. Consultar portales de internet de los fabricantes de Software instalados en la plataforma tecnológica de la Institución (Sistemas Operativos, Antivirus, Aplicaciones, Driver, Utilitarios, etc.) instalados en la plataforma tecnológica de la Institución.
2. Recibe boletines y/o correo electrónico sobre aviso de nuevas versiones de software.
3. Consultar con los representantes de Software de los programas instalados en la plataforma tecnológica de la Institución.
4. Actualizar los repositorios de actualizaciones de productos de software instalado en los servidores, a través de actualizaciones automáticas y/o batch.
5. Instalar y comprobar el funcionamiento de las actualizaciones en ambiente de prueba.
6. Generar reporte recomendando la instalación o no de la actualización en ambiente de producción.

Implementación de Actualizaciones:

1. Desinstalar actualizaciones de ambiente de prueba y documenta los datos de la misma.
2. Instalar las actualizaciones en Servidores en Producción, si es necesario.
3. Instalar y/o distribuye (Deploy) las actualizaciones en los terminales conectados a la red de datos de la Institución, si es necesario.
4. Actualizar documentación sobre actualizaciones.

Protección contra códigos maliciosos:

Se deben implementar controles de detección, prevención, recuperación y concientización, con el fin de que los usuarios tengan protección ante la presencia de algún código malicioso. En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, solo se permite la instalación de software con licenciamiento apropiado y acorde con la propiedad intelectual.

ACTUALIZACION DE CONSOLA EPOLICY DE LA SUITE MCAFEE

1. Conectar al site de McAfee (automáticamente, o por petición).
2. Actualizar componentes de la consola McAfee (motores, archivos de definición de virus, complementos, etc.).
3. Distribuir actualizaciones a las terminales (Automáticamente).
4. Aplicar actualizaciones batch en aquellos equipos que la actualización no se aplicó.
5. Verificar que la actualización se aplique a todos los equipos.
6. Actualizar registro de control de actualizaciones de software.

DISEÑO DE SOFTWARE (APLICACIONES)

1. Recibir solicitud con requerimientos de la nueva aplicación desde el departamento solicitante.
2. Registrar la solicitud en el portafolio de aplicaciones pendiente de estudio y desarrollo.
3. Autorizar el estudio para el Análisis de la aplicación solicitada.
4. Realizar levantamiento de información sobre las necesidades y requerimientos del sistema (documentos, procesos, flujo de datos, etc.).
5. Realizar estudio de Factibilidad para la aplicación.
6. Realizar recomendaciones para Diseño de la nueva aplicación.
7. Diseñar la Base de Datos para la nueva aplicación.
8. Diseñar las Entradas, Salidas, Reportes, Controles, etc.
9. Escribir los programas en el lenguaje de programación seleccionado de acuerdo al Diseño realizado.
10. Probar la aplicación con datos de prueba y datos reales.
11. Elaborar estrategia de implementación.

12. Autorizar la instalación de la aplicación a los usuarios que la utilizarán.
13. Instalar la aplicación autorizada.
14. Entrenar a los usuarios de la nueva aplicación en el uso de la misma.
15. El encargado de TIC Supervisa todas las etapas del Proyecto.

MODIFICACION SOFTWARE (APLICACIONES)

1. Recibir solicitud para agregar, modificar, eliminar, o rediseñar alguna funcionalidad de una aplicación existente.
2. Registrar la solicitud en el portafolio de aplicaciones pendiente de modificación.
3. Autorizar el estudio para el Análisis de los cambios solicitados para la aplicación.
4. Realizar levantamiento de los datos necesarios para llevar a cabo las modificaciones solicitadas.
5. Realizar estudio de Factibilidad, si es necesario.
6. Realizar recomendaciones y/o informa sobre las implicaciones de aplicar las modificaciones solicitadas.
7. Autorizar ejecución de los cambios solicitados.
8. Diseñar aplicación, si es necesario.
9. Modificar los programas necesarios.
10. Probar los programas ya modificados en ambiente de prueba.
11. Autorizar la instalación del ejecutable actualizado de la aplicación modificada.
12. Actualizar el registro de Control de Versiones para aplicaciones.
13. Entrenar a los usuarios de la nueva aplicación en el uso de la misma.
14. Supervisar todas las etapas del proceso.

POLÍTICA DE MANEJO Y PROTECCIÓN DE LA INFORMACIÓN:

Todos los usuarios de equipos de TI así como los empleados en general tienen la obligación de salvaguardar la información de la Institución, para garantizar la disponibilidad, confidencialidad y respaldo de la misma.

La preservación de la confidencialidad, asegurando que solo quienes estén autorizados pueden acceder a la información; integridad, en cuanto a que la información y sus métodos de proceso son exactos y completos; y, disponibilidad, en cuanto a garantizar que solo los usuarios autorizados tienen acceso a la información y a sus activos asociados, cuando lo requieran.

Carpetas compartidas:

Los usuarios manejaran una carpeta compartida por área, la misma solo tendrá permiso para cada empleado que trabaje en dicha área, nadie más tendrá acceso a los documentos ahí emitidos, dentro de la carpeta cada usuario puede tener acceso y modificar, por ende solo debe servir como flujo de información, no como fin de guardar documentación terminados, para eso existe una carpeta con el nombre del usuario la cual estará al igual que la común direccionada al servidor.

Carpetas de datos a usuario:

El usuario debe tener en su escritorio una carpeta con la primera letra de su nombre y el apellido la cual estará re direccionada al servidor, esa carpeta es la que ayudara al usuario a salvaguardar su información en caso de que le suceda algo a su pc, dichos datos serán recuperados de inmediato ante cualquier eventualidad sin presentar ningún contra tiempo pues estará direccionado al servidor.

Políticas y procedimientos para la elaboración de backup

1. Determinar data a la cual se le hará backup.
2. Ejecutar aplicación de backup Data Protector.
3. Configurar el programa Data Protector con las opciones adecuadas para hacer el backup de los datos requeridos.
4. Verificar que el bakckup se realizó correctamente. Hacer revisión de integridad.
5. Se envía el backup realizado a través del data protector por medio a un ftp en un almacenamiento externo en la nube

RECOMENDACION PARA COMPRA DE EQUIPOS INFORMATICOS

1. Solicitud de equipo recibida informalmente.
2. Recibir Solicitud de recomendación técnica para compra equipo desde la Dirección Administrativa.
3. El encargado de TI en conjunto con los soportes, evalúa el requerimiento tomando en cuenta las capacidades de hardware y software que necesita el usuario, así como factores tales como tendencia tecnológica, espacio físico disponible para el equipo, estándares medioambientales y energéticos, etc.
4. Remitir a la Dirección Administrativa la recomendación técnica de lugar.

VERIFICACION DE EQUIPOS Y/O SUMINISTROS INFORMATICOS ADQUIRIDOS:

1. Recibe la solicitud de verificación de equipos y/o suministros informáticos adquiridos.
2. Realizar la verificación del o los equipos adquiridos, o procede a delegar al Soporte I, la realización de la misma - en los casos que aplique.
3. Firmar el conduce de los equipos recibidos, conjuntamente con un representante de la Gerencia de Revisión y Análisis, un representante de la Contraloría y el Encargado de Suministro.
4. Remitir informe al Departamento de Compras, sobre la verificación realizada.

USO DE LAS REDES:

La dirección de TIC es el responsable de administrar, definir, ajustar y mantener el buen uso y funcionamiento de las Redes, así como administrar el ancho de banda necesario para cada servicio.

El uso de las redes será monitoreado con la finalidad de ajustar y planificar la capacidad que debe ser asignada a cada servicio, de acuerdo al desempeño que manifieste cada proceso, para con ello reducir los riesgos de posibles fallas.

Ante cualquier falla en las redes, la dirección de TIC tiene la obligación de hacer contar a su superior inmediato de acuerdo a la jerarquía, los fallos presentados, la resolución del problema y el costo probable para reparar posible falla antes de que la misma ocurra.

Telefonía fija: La asignación de extensiones telefónicas y modificación de categorías de acceso telefónico se hará de acuerdo a la solicitud del encargado del departamento con la supervisión del área de TIC poniendo en constancia que el usuario indicado está apto para dicha asignación. El uso de los teléfonos fijos asignados a los colaboradores debe ceñirse al desarrollo de actividades relacionadas con el cargo.

Toda avería o conflicto con dicha extensión debe ser reportada al área de TIC, dando detalles del problema presentado, dicha área debe acudir a dar resolución al problema reportado.

En caso de mal uso a dicha extensión, el soporte encargado de revisión de la avería debe de notificar a su supervisor inmediato para fines de reporte a la persona indicada.

Estándares de la Política para equipos portátiles y dispositivos móviles. Asignación y uso de teléfonos celulares:

El departamento debe hacer solicitud de asignación de flota a la persona que va a darle utilidad, luego la dirección de TIC se encarga de hacer la solicitud de aprobación a la máxima autoridad, para luego de ser aprobada proceder a la entrega de la misma.

La asignación de los equipos y planes de telefonía celular para los empleados de la Institución se realiza de acuerdo con el cargo que ocupe y con la solicitud enviada por el encargado de departamento al cual pertenece.

La responsabilidad de dicho equipo queda totalmente designada a la hora de la entrega a la persona que recibe, por igual deben dar un uso racional y estrictamente laboral, el uso de minutos asignados también será por fechas establecidas.

En caso de que la persona no le de abasto la cantidad de minutos asignada, deberá de emitir una comunicación al área de TI, firmada y autorizada por su supervisor inmediato.

ASISTENCIA DIRECTA:

Son las asistencias dadas al usuario que solicita un soporte ya sea vía telefónica como por teléfono pero requiriendo la presencia del soporte técnico en el departamento.

1. Levantamiento de reporte por parte del usuario, inicia creando el ticket en el CRM.
2. Asistir al llamado y ver el problema reportado
3. Establecer el diagnóstico del problema presentado.
4. Implementar la solución al diagnóstico anteriormente dado si existe.

5. Dar seguimiento a la efectividad de la solución.
6. Cierre de ticket.

ASISTENCIA TELEFONICA:

1. Levantamiento de reporte por parte del usuario, inicia creando el ticket en el CRM.
2. Establecer diagnóstico del problema presentado por el usuario por medio a dicha vía.
3. Indicar al usuario la solución al problema reportado, por medio a los pasos a realizar para resolver dicho problemas, si el usuario lleva a cabo todo el procedimiento para la solución y no fue efectivo, el soporte debe iniciar en el paso 2 de la asistencia directa.
4. Si la solución fue hallada vía telefónica se hace cierre del ticket.

REPARACIÓN INTERNA DE EQUIPOS INFORMATICOS:

- 1- Recepción y Registro de Reporte de Avería en Equipo Informático.
- 2- Registro del reporte de avería.
- 3- Trasladar el equipo al taller interno de TIC.
- 4- Realizar evaluación y diagnóstico de la avería reportada.
- 5- Informar al director de TIC sobre el problema presentado.
- 6- Transferir a proceso de reparación de avería en taller externo, si es necesario.
- 7- Solicitar piezas al director de TIC, si es necesario.
- 8- Solicitar piezas existentes al almacén, y/o Gestionar la compra de otras, si es necesario.
- 9- Instalar piezas.
- 10- Probar el equipo, verificando que el mismo esté funcionando correctamente e informar al director de TIC.
- 11- Entregar el equipo reparado al usuario.
- 12- Cierre caso de avería.

REPARACIÓN EXTERNA DE EQUIPO INFORMATICO:

1. Emitir reporte de evaluación de Equipo de la Unidad de Soporte indicando que no se puede reparar el equipo en el taller interno.
2. Solicitar a la Dirección Administrativa autorización para enviar el equipo a taller externo para fines de evaluación y/o reparación.
3. Recibir autorización aprobada y Gestionar la salida del mismo hacia taller externo.
4. Actualizar el registro de la avería haciendo constar que será reparado en taller externo.
5. Gestionar el envío equipo al taller externo.
6. Recibir cotización sobre el costo de la reparación.
7. Determinar factibilidad de la reparación.

8. Solicitar autorización a la Dirección Administrativa para que el taller externo proceda a reparar el equipo según cotización.
9. Recibir aprobación de reparación y se notifica al taller externo que proceda con la reparación.
10. Recibir equipo reparado por parte del taller externo.
11. Probar el equipo, verificando que el mismo esté funcionando correctamente e informa al director de TIC.
12. Supervisar que la avería haya resuelta.
13. Entregar el equipo reparado al usuario.
14. Cierre caso de avería.

Mantenimiento de equipos:

Es el proceso a realizar a todos los equipos de TIC utilizado por los usuarios de la Institución, los mismos están distribuidos por departamentos, estos equipos mantienen un control en la dirección de TIC desde la adquisición hasta su culminación de descarga por daños o desactualización, todos son registrados y modificados en el formulario manejado para fines de seguimiento.

En el manual de mantenimiento correctivo y preventivo se presentan los pasos a elaborar el proceso de mantenimiento dados a continuación:

Preventivo:

1. Realizar levantamiento de los equipos a realizar el mantenimiento por planta y departamento.
2. Realizar las pruebas de software y hardware para fines de diagnósticos.
3. Llevar equipo al área de TIC para limpieza interna y externa.
4. Realizar limpieza física interna y externa, utiliza herramientas de software para mantenimiento lógico del equipo (borrado de temporales, desfragmentación de disco, desinstalación de aplicaciones maliciosas, actualización de antivirus, actualización de sistema operativo, actualización de aplicaciones, etc.), formatea el equipo si es necesario y se le instalan todos los recursos de hardware y software que utiliza el usuario al que está asignado el equipo.
5. Terminado dicho proceso y registrado el mantenimiento, así como la revisión del formulario general de equipos, se procede a la entrega de equipo al lugar correspondiente.
6. Instalar equipo en su ubicación de origen.
7. Asistencia Cerrada.

Correctivo:

1. Levantamiento de información de equipos que han presentado problemas.
2. Realizar las pruebas de software y hardware de lugar.
3. Llevar el equipo al área de TIC.
4. Reemplazar hardware requerido o actualizar e implementar software requerido.
5. Instalar equipo en su ubicación de origen.
6. Asistencia Cerrada.

MANTENIMIENTO DE BASE DE DATOS:

1. Consultar calendario de mantenimientos y da seguimiento al mismo.
2. Recibir reporte de error en uno de los sistemas conectados a la base de datos de la Institución.
3. Realizar backup de la Base de Datos.
4. Ejecutar las operaciones de mantenimiento estándar (reducción de logs, reparación de tablas, índices, recomposición de data corrompida).
5. Realizar tareas de programación, si es necesario.
6. Restaurar Base de Datos, si es necesario.
7. Supervisar la realización de los procesos de mantenimiento.

ASIGNACION DE ACCESO A RECURSO INFORMATICO:

1. Recibir comunicación de solicitud de acceso a recurso informático.
2. Registrar solicitud en Sistema de Administración de Documentos.
3. Determinar la pertinencia de la solicitud.
4. Realizar conexión con Servidor o Terminal, si es necesario.
5. Ejecutar software necesario para otorgar el acceso solicitado.
6. Asignar los derechos a acceso necesarios de acuerdo a la solicitud.
7. Actualizar registro de Acceso a Recursos Informáticos.
8. Informar al solicitante, y requerir firma de documento en la que el usuario se responsabiliza por los eventos que ocurran a su nombre en el recurso al que se le ha otorgado acceso.

CREACION DE USUARIO DE WINDOWS:

1. Recibir comunicación de solicitud de creación de usuario indicando quién será el titular del mismo.
2. Registrar solicitud en Sistema de Administración de Documentos.
3. Determinar la pertinencia de la solicitud.
4. Realizar conexión con el Servidor "Active Directory".

5. Ejecutar Active Directory y completa los parámetros necesarios.
6. Asignar el usuario a uno de los grupos definidos de la institución, si aplica.
7. Actualizar registro de Usuarios.
8. Informar al solicitante, y requerir firma de documento en la que el usuario se responsabiliza por los eventos que ocurran a su nombre.

Actualización y Reseteo de Clave usuario.

1. El usuario debe solicitar el cambio de contraseña en caso de sospechar que alguien más está dándole utilidad
2. La contraseña puesta por el usuario tiene un tiempo vigente de 30 días, la misma de manera automática le pedirá cambio, cambio que tendrá que ser realizado o el sistema no dejara acceder a la pc.
3. La clave es un patrón único que solo debe ser manejado por dicho usuario propietario de la misma, si de alguna manera la persona infringe en suministrar usuario y clave a más personas, cualquier evento ocurrido bajo su usuario queda bajo su responsabilidad.
4. La clave debe tener mínimo ocho caracteres, la primera letra mayúscula, no debe ser su nombre, ni la clave anterior puesta.

INSTALACION DE PROGRAMA INFORMATICO:

1. Recibir comunicación solicitando la instalación de un programa o aplicación ausente en el equipo del solicitante.
2. Registrar solicitud en Sistema de Administración de Documentos.
3. Determinar la pertinencia de la solicitud.
4. Realizar evaluación al equipo para ver si cumple con los requisitos del programa que se desea instalar.
5. Instalar programa solicitado.
6. Instruir al usuario sobre aspecto general de uso del programa.
7. Informar al director de TIC.
8. Actualizar registro de Usuarios de Programas.

MONITOREO DE PLATAFORMA TECNOLOGICA:

1. Gestionar la compra software y/o hardware necesario para monitoreo de los recursos informáticos.
2. Configurar y/o solicita la configuración a terceros de hardware y/o software de monitoreo de recursos informáticos.
3. Realizar evaluación al equipo para ver si cumple con los requisitos del programa que se desea instalar.

4. Producir reporte periódicos a partir de las herramientas de monitoreo.
5. Programa alertas.
6. Informar a Usuarios y Autoridades de la Institución sobre la ocurrencia de eventos importantes detectados.
7. Registrar los eventos para fines actualizar fuente de conocimientos previos y para fines estadísticos.

Recursos Manejados en el área de Seguridad:

La seguridad de la información protege la información de un rango de amenaza y garantiza la continuidad del negocio. Hay que evitar que las amenazas atenten contra la continuidad del negocio

La seguridad del negocio tiene 3 aspectos fundamentales que son:

1. **La confidencialidad:** donde se garantiza que la información será accedida por las personas autorizadas
2. **La integridad:** que es que la información sea correcta y completa, y su procesamiento sea correcto de acuerdo a lo establecido.
3. **Disponibilidad:** que los usuarios puedan acceder a la información donde y cuando se le requiera.

Tomando en cuenta que la seguridad de la información es responsabilidad de todo desde la persona que cuida la entrada hasta la máxima autoridad del INVI (Instituto Nacional de la Vivienda) Estamos comprometido con la seguridad de la información.

Lo que no lleva a Los recursos que empleamos para estos fines, los cuales son Humano, físicos, monetario y tecnológico los cuales empleamos de la siguiente Forma.

Contamos con un excelente equipo operacional, además de las herramientas para hacer un buen trabajo además

Contamos con: más de 250 computadoras debidamente equipadas con las aplicaciones necesarias para el trabajo.

Seguridad física, seguridad digital, equipos para respaldo, personal capacitado, conjunto de aplicaciones para realizar el trabajo, antivirus, cableado estructurado, unidades de copia de respaldo.

En las Instalaciones principal y en todas las sucursales tenemos apoyo militar para el control de acceso a la institución, los cuales se encargan de conducir a los visitantes al personal de protocolo que se encuentran en la resección del primer piso; En todos los pisos tenemos apoyo militar, y el personal de protocolo, quienes a su vez de asistir a la visitas, verifican que los empleados estén Bien Identificados

- El personal de protocolo solicita una identificación y procede a registrar en el sistema de visita donde registra el lugar y la persona que el visitante vine a visitar y le identifica con un label con los datos pertinentes. Y al retirarse entregan el label y le entregan su documento.
- Si personas internas como externa solicitan una información que no es de su dominio, tiene que hacerlo a través de la autorización de una persona que si tenga esa autoridad después de validar para cuales fines es necesaria. Y si es una persona externa tiene que canalizarlo a través del departamento de libre acceso a la información pública.
- Las instalaciones constan con un sistema de vigilancia Digital con más de 28 cámaras de seguridad distribuidas en lugares estratégicos de más vulnerabilidad.
- Las instalaciones cuentan con un sistema contra incendio distribuido por toda la instalaciones, además eta equipada con diferente tipos de extintores de acuerdo a las exigencia del Área
- Toda la información crítica están en las instalaciones principales la cual esta alojadas en diferentes servidores, los cuales están en un data center debidamente climatizado, conectado con un ups independiente y con una redundancia o backcup a los ups generales y con una planta de emergencia que entra automático en lo que encienden la panta principal o se normaliza la energía contratada.
- En el data center tenemos varios storage de almacenamiento y le sacamos copia de respaldo diario a toda la data critica local, externa y en la nube, además que periódicamente lo hacemos con toda la data incluyendo réplicas de los escenarios virtuales. Los que nos garantiza la continuidad del negocio en cualquier eventualidad.

El data center consta con uno de los más avanzado equipos de FortiGate:

- Para garantizar la seguridad de la red, además un servicio de antivirus con unas de las más prestigiosas compañías que ofrecen servicios empresariales.
- Tenemos 5 gabinetes de red con múltiples switch de red debidamente protegidos tanto en el espacio como el gabinete tiene llaves y en general serian 8 gabinetes con los 3 que están en el Datacenter donde se alojan los switch principales, los equipos de comunicaciones, los NVR de las cámaras de seguridad, los equipos de conectividad con la sucursal de Santiago y los servidores.

Asignación de los Roles Especifico y responsabilidad en seguridad informática en la organización.

Seguridad Física: La seguridad física es responsabilidad del director de seguridad militar con su equipo.

Seguridad Logísticas: Es responsabilidad del departamento de protocolo y su equipo.

Seguridad TIC: Es responsabilidad de la Dirección de tecnología con sus diferentes dependencias principalmente el encargado de seguridad de TIC.

Lo que indica que al final todos los empleados que trabajan para el INVI son responsable de la información que la institución ha confiado en sus manos para ser administrada, pues del buen uso de la misma depende la seguridad, la integridad de la información y de la institución.

Concientización al personal sobre Seguridad E implementación de los controles de Seguridad Informática:

A fines de que todas las áreas de la Institución conozca sobre algunas precauciones y colaborar con la manera de manejar los datos de cada uno, nos encargamos de establecer parámetros claros con cada una de ellas, hemos enviado circulares dando explicaciones y parámetros de la forma en que pueden darle acceso a intrusos a nuestros servidores a través de cualquier medio de transporte de información, dígame: correo, **memorias, mensajes no identificados, etc.**, de igual manera hemos proporcionado espacios en nuestro servidores donde el usuario guarde sus documentos de trabajo con la salvedad que fuera de ahí si al equipo llegase a sucederle algo y no estar en esa dirección, no es 100% seguro recuperar la misma.

En cuanto a seguridad de usuario, se le indica al usuario que para poder utilizar una pc que le haya sido asignada debe su supervisor inmediato enviar una comunicación al área de TIC solicitando la creación de usuario y los permisos que este tendrá, a cuales sistemas tendrá acceso? y que manejará?, luego de haber recibido dicha comunicación, el departamento de TIC se encarga de hacer la creación de dicho usuario en el área de servidores con todas las políticas de restricción o permiso que haya sido solicitada, después de ese procedimiento se le informa al supervisor y al usuario por medio a una comunicación que su solicitud ha sido realizada.

Estos controles de acceso a los usuarios permiten tener una ventaja exorbitante para la seguridad en el área de TIC, por eso mantenemos el protocolo de seguridad, a fines de dar cumplimiento a los estándares.

“Año de la Innovación y la Competitividad”

Marte 22 de Octubre, 2019

Circular

A TODO EL PERSONAL



Cortésmente le informamos que El Equipo Nacional de Repuestas a Incidentes Cibernéticos (CSIRT-RD) ha identificado una campaña de spam a través de correos electrónicos que distribuye malware utilizando macros en archivos de Microsoft Word, la extensión utilizada en dichos correos es **.doc.**, utilizan **asuntos** del tipo: **“Reclamación...”**, **“quejas ..”** **Plan de acción complementario o Asesoramiento de pagos de remesas.**

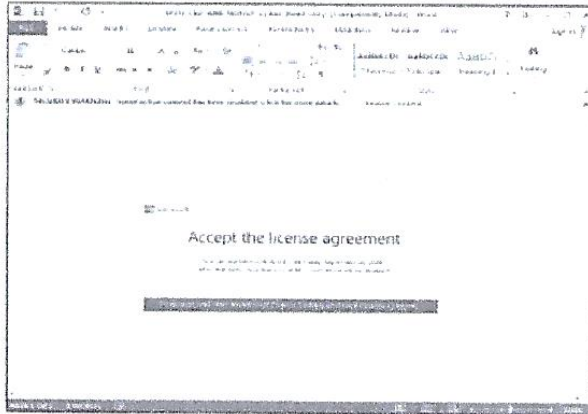
EMOTET es un troyano bancario que fue identificado por primera vez en el 2014. Diseñado inicialmente como un malware que intentaba ingresar en los ordenadores y robar información confidencial y privada. Posee capacidades similares a los gusanos para su propagación.

Es polimórfico, lo que significa que puede cambiar por sí mismo cada vez que se descarga y evita la detección basada en firma.



Si a su correo llega algún documento el cual usted no conoce el destinatario cohíbese de abrir dicha información.

El documento de Word emplea técnicas de ingeniería social para convencer a los usuarios que habiliten la ejecución del proceso malicioso.

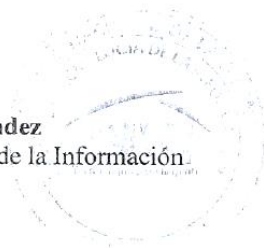


NOTA: En caso de detectar algún posible equipo infectado será retirado del lugar para fines de chequeo y aislamiento de la red, evitando el posible contacto con otros equipos, para los fines el equipo infectado no será devuelto al usuario hasta no descartar daños causados.

Agradecemos su colaboración en este proceso, para evitar posibles infecciones entrantes por vía de usuarios, sin nada más por el momento, se despide,

Ing. Juan Hernández

Enc. Departamento Tecnología de la Información



JH/mr.-

“Año de la Innovación y la Competitividad”

Martes 21 de Mayo, 2019

Circular

A TODO EL PERSONAL

Cortésmente le informamos que no somos responsables de los documentos que sean guardados fuera del acceso directo de su computador ya que se le ha reiterado en varias ocasiones el buen uso de la integridad a la seguridad de la misma, haciendo constar que queda bajo su responsabilidad cualquier documentación guardada fuera de este.

Agradecemos su colaboración en este proceso, sin nada más por el momento, se despide,



Ing. Juan Hernández

Enc. Departamento Tecnología de la Información

JH/yf.-



INSTITUTO NACIONAL DE LA VIVIENDA

"Año del fomento de las exportaciones"

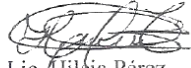
26 de febrero de 2018

Al : **Ing. Juan Hernández**
Encargado de Tecnología de la Comunicación

Asunto : Solicitud correo electrónico

Cortésmente, le solicitamos crear el correo institucional cep@invi.gob.do para uso de la Comisión de Ética de la Institución, a fin de cumplir con las actividades encomendadas en el desarrollo de sus funciones.

Muy Atentamente,


Lic. Hilcia Pérez
Coordinadora General
CEP-INVI



Jueves 22 de Marzo, 2018

DTI-0452-2018

A : Ing. Eleazar Parra Guerra
Enc. División de ingeniería y Presupuesto

Asunto : Respuesta a solicitud

Anexo : Copia Comunicación DIP-25-2018

Cortésmente, le informamos que el usuario solicitado por usted en la comunicación DIP-25-2018 d/f 20/03/2018, ha sido realizado.

Credenciales del usuario:

Sistema	Usuario	Titular Cuenta	Clave
Windows	Eparra	Eleazar Parra Guerra	Invi2020

- Al ingresar por primera vez al sistema; el usuario autoriza al Departamento de Tecnología a monitorear las actividades realizadas por el titular de la cuenta en la infraestructura informática del Invi.
- “Todas las acciones de los usuarios son registradas automáticamente en nuestros servidores, para fines de establecer responsabilidades”.

Responsabilidades directas del Titular

- ✚ Cambiar la contraseña la primera vez que ingrese al sistema.
- ✚ Responder por TODO lo que se haga en los recursos informáticos del Invi utilizando dichas credenciales.
- ✚ Solicitar cambio de contraseña cuando sospeche que alguien se le ha copiado.
- ✚ Cerrar o bloquear su sesión cuando no se encuentre frente al computador.
- ✚ Otras.

Sin nada más por el momento, se despide,


Ing. Juan Hernández

Enc. Departamento Tecnología de la Información.

JH/yf

Rosaily Victoria
22/03/2018

Teléfono: 809-732-0600
Fax: 809-227-5803
Correo Electrónico: info@invi.gob.do
Av. Pedro Henríquez Ureña
Esa. Av. Alma Mater, Santo Domingo,
República Dominicana

f INVI t INVI i INVI



INSTITUTO NACIONAL DE LA VIVIENDA

"Año del Fomento de las Exportaciones"

DIVISION DE INGENIERIA Y PRESUPUESTO.

DIP-25-2018

Santo Domingo, R.D.
20 de marzo del 2018

AL : **ING. JUAN HERNANDEZ**
Enc. De Tecnología

VIA : **ING. RENSO CUEVAS.**
Gerente Construcción y Proyectos

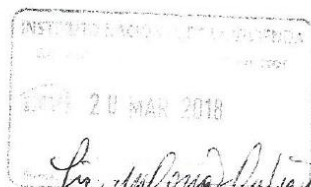
ASUNTO : **Solicitud Usuario.**

Cortésmente, por medio de la presente, le estamos solicitando la creación de usuario para el Ing. Eleazar Parra Guerra, Enc. De la División de Ingeniería y Presupuesto, para los fines correspondiente, esperando su pronta respuesta.

Sin otro particular,

Atentamente,

ING. ELEAZAR PARRA GUERRA
Encargado División de Ingeniería y Presupuesto





INSTITUTO NACIONAL DE LA VIVIENDA

INSTITUTO NACIONAL
DE LA VIVIENDA

"AÑO DEL FOMENTO A LAS EXPORTACIONES"

GERENCIA DE CONSTRUCCION Y PROYECTOS

GCP/946-18

11 de Septiembre del 2018

AL : **LIC. JUAN HERNANDEZ**
Encargado de Informática.

ASUNTO : **Solicitud de Instalación de AutoCAD y Usuarios.**

Cortésmente, por medio de la presente tenemos a bien solicitarle la Instalación del Programa **AutoCAD** para la **Ing. Maritza Leguizamón**, Encargada de la División de Supervisión Eléctrica de esta Gerencia y a su vez la Creación de Usuarios al **Ing. Feliz Ruiz** y al **Sr. Wilmer Cepeda Solís**, ayudantes de esa división. Hacemos dicha solicitud para su conocimiento y fines de lugar.

Sin otro particular,

Atentamente,


ING. RENSO BDO. CUEVAS P.
Gerente de Construcción y Proyectos

RBCP/mjb

Teléfono: 809-732-0600
Fax: 809-227-5803
Correo Electrónico: info@invi.gov.do
Av. Pedro Henriquez Ureña
Esq. Av. Alma Mater, Santo Domingo,
República Dominicana

 INVI RD  INVI_RD  INVI_RD

Seguridad Física y medios de acceso:



"AÑO DE LA INNOVACIÓN Y LA COMPETITIVIDAD"

21 de noviembre del 2019
Santo Domingo, D.N.


A TODO EL PERSONAL

Cortésmente, por medio de la presente les informamos que los funcionarios que aparecen en este listado son los que están autorizados para entrar por la parte trasera de la institución (Área de la Seguridad Militar).

- **Licda. Yanira Agramante** (Directora Administrativa)
- **Licda. Mayerlin Jorge** (Directora de Recursos Humanos)
- **Licda. Yohana Minaya** (Asistente del Director General)
- **Lic. Rafael Tertulien** (Director financiero)
- **Ing. Ramón Shuede** (Director de Planificación Y Desarrollo)
- **Dr. Mario Jacob** (Director Social)
- **Ing. Renso Cuevas** (Director de construcción y Proyectos)
- **Dr. Bernardo Jiménez** (Director Jurídico)
- **Ing. Juan Hernández** (Director de Tecnología)
- **Lic. Antonio Victorio** (Encargado de Programa de Estufas y Tanques)
- **Lic. Franklin Pacheco** (Encargado de Programas Sociales)
- **Sr. Francisco Peña** (Encargado de Compras)

Sin otro particular, se despide,

Atentamente,


Licda. Mayerlin Jorge
Directora Interina de Recursos Humanos



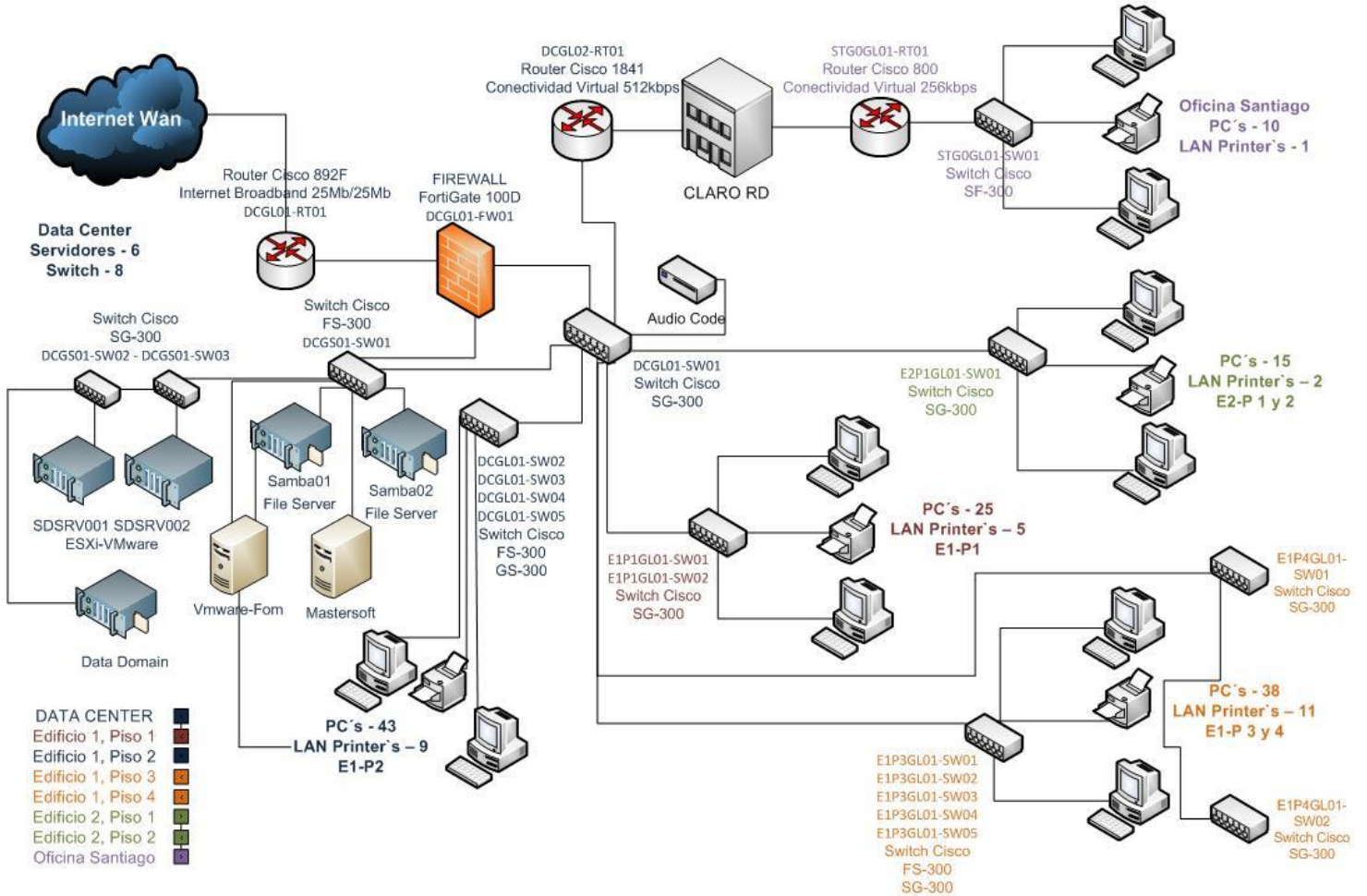
Teléfono: 809-712-0900
Fax: 809-227-5803
Correo Electrónico: info@invi.gob.do
Av. Pedro Henríquez Ureña
Esq. Av. Abra Mater, Santo Domingo,
República Dominicana

📞 📠 📧 🌐

Infraestructura de Hardware (Equipos, Dispositivos, Aparatos)

Diagrama de Red:

Diagrama de Red División Tecnología INVISD



Edificio Principal, Primer Piso (E1P1GL01)

Ítem	Marca	Modelo	Nombre ID	Comentario
Gabinete de Pared	n/a	n/a	E1P1GL01	
Patch Panel 24/pts.	Quest	n/a	PP-1	
Patch Panel 24/pts.	Quest	n/a	PP-2	
Organizador	Quest	n/a	Organizador	
Organizador	Quest	n/a	Organizador	
Switch 28/pts.	Cisco	SG-300	E1P1GL01-SW01	
Switch 28/pts.	Cisco	SG-300	E1P1GL01-SW02	

Edificio Principal, Depto. Informática (DCGL01)

Ítem	Marca	Modelo	Nombre ID	Comentario
Gabinete Vertical	HP	n/a	DCGL01	
Patch Panel 96/pts.	Quest	n/a	PP-1	
Patch Panel 96/pts.	Quest	n/a	PP-2	
Organizador	Quest	n/a	Organizador	
Organizador	Quest	n/a	Organizador	
Switch 28/pts.	Cisco	SG-300	DCGL01-SW01	
Switch 28/pts.	Cisco	SG-300	DCGL01-SW02	
Switch 24/pts.	Cisco	FS-300	DCGL01-SW03	
Switch 24/pts.	Cisco	FS-300	DCGL01-SW04	
Switch 24/pts.	Cisco	FS-300	DCGL01-SW05	
Router	Cisco	892F	DCGL01-RT01	
Firewall	Fortinet	Fortigate 100D	DCGL01-FW01	
Audio Code	Meridiant	500 MSBR	DCGL01-PBX	

Edificio Principal, Depto. Informática (DCGL02)

Ítem	Marca	Modelo	Nombre ID	Comentario
Gabinete Vertical	HP	n/a	DCGL02	
Router	Cisco	1841	DCGL02-RT01	
Servidor	Hewlet Packard	HP ProDesk	VMWARE-FOM	VMWare Player, HP Store Virtual Mngr

Edificio Principal, Depto. Informática (DCGS01)

Ítem	Marca	Modelo	Nombre ID	Comentario
Gabinete Vertical	HP	n/a	DCGS01	
Switch 24/pts.	Cisco	FS-300	DCGS01-SW01	
Switch 24/pts.	Cisco	GS-300	DCGS01-SW02	
Switch 24/pts.	Cisco	GS-300	DCGS01-SW03	
Servidor	HP ProLiant	DL380 G9	SDSRV001	VMWare
Servidor	HP ProLiant	DL380 G9	SDSRV002	VMWare
Servidor	Dell	745	Samba02	File Server
Servidor	Dell	9010	Samba01	File Server
Data Domain	Dell	Dell EMC2	DD2200	Data Protector
Servidor	Dell	5040	SRVA	Mastersoft
Servidor	HP ProLiant	DL360 G7	SRVPDC	Domain Control

Edificio Principal, Tercer Piso (E1P3GL01)

Ítem	Marca	Modelo	Nombre ID	Comentario
Gabinete de pared	n/a	n/a	E1P3GL01	
Patch Panel 24/pts.	Quest	PP-1	PP-1	
Organizador	Quest	n/a	Organizador	
Organizador	Quest	n/a	Organizador	
Organizador	Quest	n/a	Organizador	
Switch 24/pts.	Cisco	FS-300	E1P3GL01-SW01	
Switch 24/pts.	Cisco	FS-300	E1P3GL01-SW02	
Switch 24/pts.	Cisco	FS-300	E1P3GL01-SW03	
Switch 28/pts.	Cisco	SG-300	E1P3GL01-SW04	
Switch 28/pts.	Cisco	SG-300	E1P1GL01-SW05	
PatchPanel 96/pts.	Quest	n/a	PP-2	
PatchPanel 48/pts.	Quest	n/a	PP-3	
Patch Panel 24/pts.	Quest	n/a	PP-4	

Edificio Banco, Primer Piso (E2P1GL01)

Ítem	Marca	Modelo	Nombre ID	Comentario
Switch 28/pts.	Cisco	SG-300	E2P1GL01-SW01	
Gabinete de Pared	n/a	n/a	E2P1GL01	
Patch Panel 24/pts.	Quest	n/a	PP-1	
Patch Panel 24/pts.	Quest	n/a	PP-2	
Organizador	Quest	n/a	Organizador	
Organizador	Quest	n/a	Organizador	

Localidad Santiago (STGOGL01)

Ítem	Marca	Modelo	Nombre ID	Comentario
Switch 24/pts.	Cisco	FS-300	STG0GL01-SW01	
Router	Cisco	800	STG0GL01-RT01	
Router	Cisco	1700	STG0GL01-RT02	
Gabinete de pared	n/a	n/a	STG0GL01	
Patch Panel 24/pts.	Quest	n/a	PP-1	
Organizador	Quest	n/a	Organizador	

Total General Servidores y Terminales conectados.

Total PC's = 207

Total Printer de Red = 76

Total Servidores:

Físico =9

Virtuales = 11

Nota:

El tipo cableado estructurado de la institución está realizado según la norma **ANSI TIA/EIA**, alambre de cobre **UTP** Categoría **5e 568-B**. Dichos enlaces entre las **IDF** están conectadas por este tipo de medio.

Detalles Distribución de la Red, Topología de Red y Equipos de Comunicación.

Internet Broadband en Fibra Óptica, ISP Codetel está configurada en un Router Cisco 829F (**DCGL01-RT01**) con una velocidad de 25Mb/25Mb, dicha WAN entrante está conectada al **FIREWALL FortiGate 100D (DCGL01-FW01)** Edificio Principal, Depto. Informática (**DCGL01**) en este equipo está configurado la WAN entrante.

Internet Broadband en Fibra Óptica, ISP Codetel está configurada en un Router Cisco 829F (**DCGL01-RT01**) con una velocidad de 25Mb/25Mb, dicha WAN entrante está conectada al **Audio Code (DCGL01-PBX)** Edificio Principal, Depto. Informática (**DCGL01**) en este equipo están configuradas todas las extensiones de la telefonía IP, a través del cual se conecta con la PBX en las nubes de Claro, quien nos suministra el servicios de voz sobre IP.

Firewall FortiGate 100D(DCGL01-FW01) está conectado al **Switch Cisco FS-300(DCGL01-SW01)**, desde aquí están conectados los enlaces y la distribución de las redes hacia los demás **IDF** que conectan las distintos Pisos y localidades de la Institución.

Switch Cisco FS-300 (DCGS01-SW01), desde este Switch están conectados el **File Server (Samba01, Samba02)**, (**SRVPDC**), (**DD2200**), Dos **Switch Cisco SG-300 (DCGS01-SW02, DCGS01-SW03)** conectado entre ellos los cuales manejan las conexiones de los dos Servidores **HP DL380 G9 (SDSRV001, SDSRV002)**, en los cuales se encuentran instalados los Servidores Virtuales que manejan los Sistemas de la Institución.

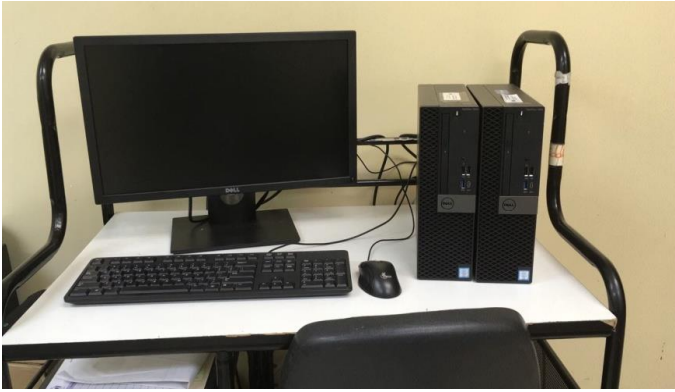
Enlace-1, desde el Edificio Principal, Depto. Informática (**DCGL01**), **Cisco SG-300 (DCGL01-SW01)**, hacia el Edificio Principal, **Primer Piso (E1P1GL01)**, el mismo está conectado al **Switch Cisco SG-300 (E1P1GL01-SW01)**, ubicado en el Edificio Principal, Primer Piso. Los cuales distribuyen las conexiones de redes a las terminales y printer del mismo piso.

Enlace-2 desde el Edificio Principal, Depto. Informática (**DCGL01**), **Cisco SG-300 (DCGL01-SW01)**, hacia el Edificio Principal, **Tercer Piso (E1P3GL01)**, el mismo está conectado al **Switch Cisco SG-300 (E1P3GL01-SW01)**, ubicado en el Edificio Principal, tercer Piso. Los cuales distribuyen las conexiones de redes a las terminales y lan printer de los pisos tres y cuatro del edificio principal.

Enlace-3 desde el Edificio Principal, Depto. Informática (**DCGL01**), **Cisco SG-300 (DCGL01-SW01)**, hacia el Switch **Cisco SG-300 (E2P1GL01-SW01)**, ubicado en el **Edificio Banco, Primer Piso**, de este están conectados los **Switch Cisco SG-300 (2P1GL01-SW01)**, EL cual distribuyen las conexiones de redes a las terminales y printer de los pisos uno y dos del edificio 2.

Conexión virtual, localidad Santiago desde el **Switch Cisco FS-300 (DCGL01-SW01)** Edificio Principal, Depto. Informática, hacia el **Router Cisco 1841 (DCGL02-RT01)**, **Conexión Virtual 512/Kbps** vía CLARO Dominicana, conectando el enlace virtual en la localidad de Santiago, en el **Router Cisco 800 (STG0GL01-RT01)**, a una velocidad de 256/kbps, este está conectado al **Switch Cisco FS-300 (STG0GL01-SW01)**, el cual distribuye las conexiones de redes a las terminales y printer de la localidad.

Computadores



Impresoras



Switch Y Teléfonos

Switch Cisco de la serie Business SG300, utilizado en la telefonía IP.



Fortigate 100



Central IP, PBX hosteada con nuestro proveedor claro

Teléfono utilizado en la nueva central por voz IP

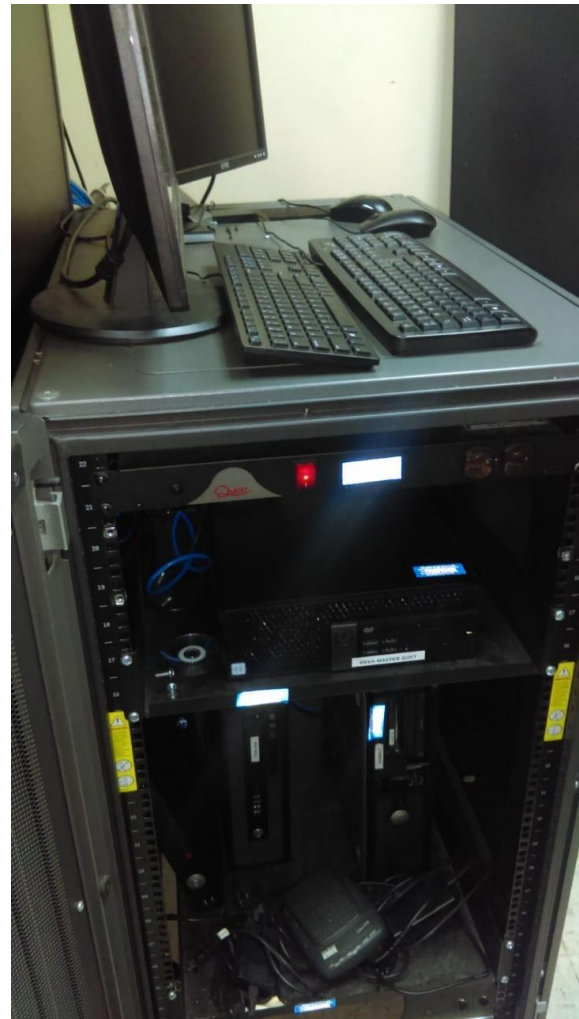


Sistema de vigilancia:

Visión de las cámaras desde el centro de monitoreo



Servidores Físicos



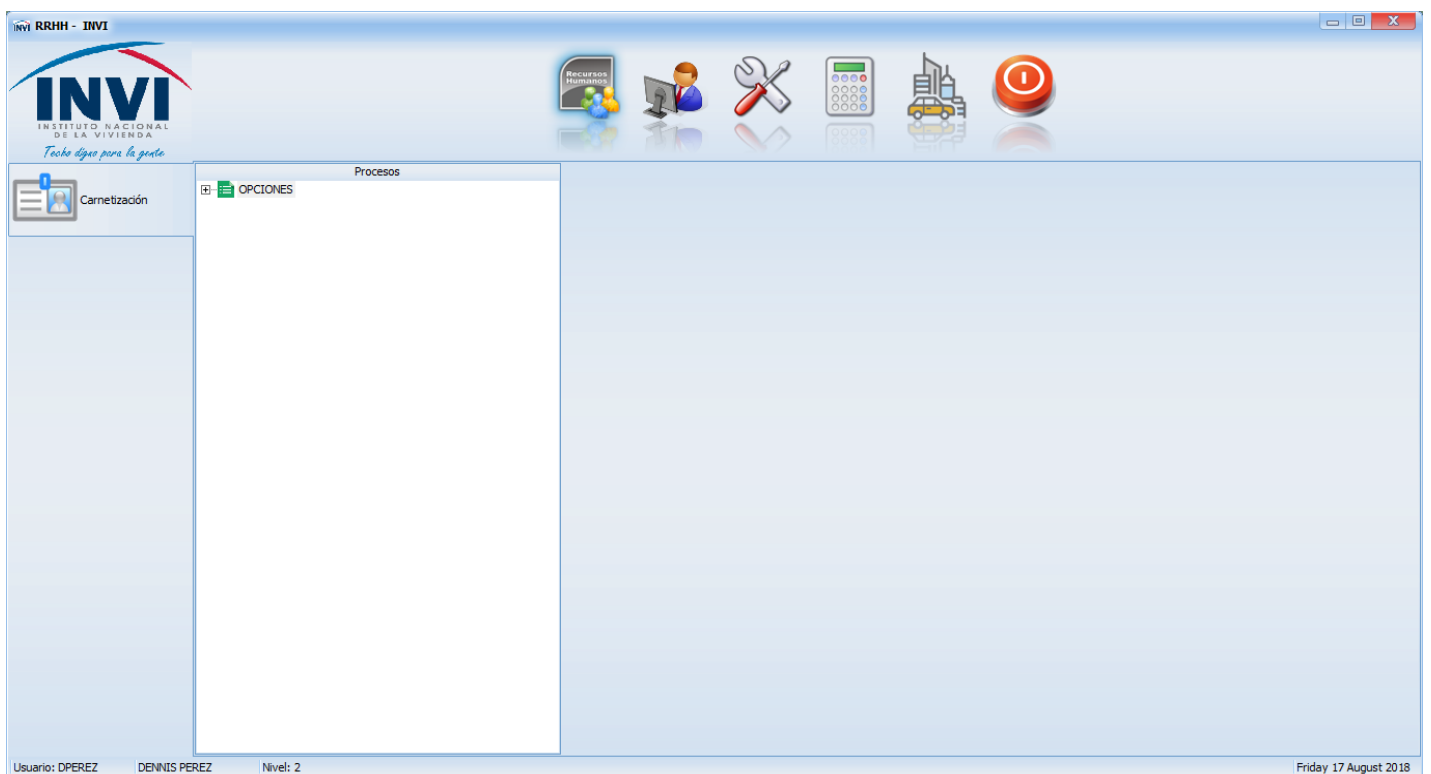
En toda organización el orden de prioridad es la data, donde los equipos físicos son reemplazables, pero la información una vez perdida, es imposible recuperar si no se tiene la copia debidamente guardada.

Infraestructura de Software:

Accesos a sistemas:



Sistema de control de acceso



Sistema de RRHH

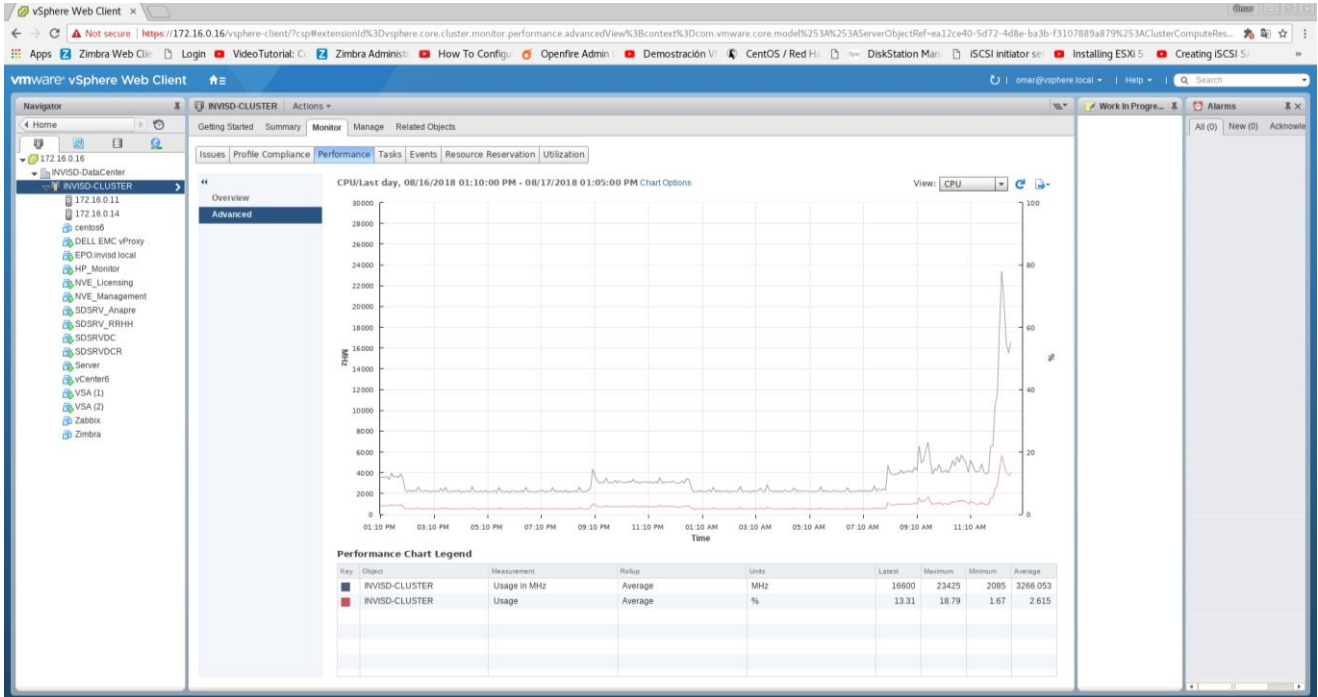


REPUBLICA DOMINICANA
INSTITUTO NACIONAL DE LA VIVIENDA
OFICINA PRINCIPAL

Sistema de Recursos Humanos
Módulo de Gestión de Personal
(Puesto en Marcha desde Diciembre 2016)



Servidores virtuales



Otros sistemas manejados:

NO	SISTEMAS UTILIZADOS EN LA INSTITUCIÓN
1	Mastersoft
2	Cartera Hipotecaria
3	Onbase
4	sistema Jurídico
5	Padrón
6	Recomi
7	Administración de Documentos
8	Tun
9	Sistema de Bono
10	Internet Bankin
11	Compra y Contrataciones
12	Sistema de Compra
13	TSS
14	DGI
15	Contabilidad Gubernamental
16	Sistema de Registro de Empleado
17	SIGO
18	SIGEF
19	Ruta(Sistema de Planificación)
20	Anapre
21	Carnetizacion
22	Sistema de Acción Rápida
23	Sistema de Almacén
24	Sistema de Pisos
25	Descuentos de Cafetería

Evaluación y Gestión de Riesgos:

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGACIÓN
					INTERNOS	EXTERNOS			
1	Resolver, por la vía telefónica, un Problema técnico que presenta un usuario.	1- Recibir, por la vía telefónica, la solicitud del servicio técnico con la necesidad expuesta por el usuario y determina si aplica para asistencia telefónica, presencial o remota.	Imposibilidad de recibir la llamada telefónica.	Central telefónica fuera de servicio.	Operativo		Dar seguimiento al calendario de mantenimiento de la central telefónica		
		2- Registrar la Solicitud del Servicio, solicitando los datos del problema presentado por el usuario.	Imposibilidad de realizar el registro digital	Recurso digital (PC y/o sistema de registro no disponible	Operativo		Realizar registro manualmente en el formulario Solicitud de asistencia técnica		

	Asigna el caso a un soporte técnico						
	3- Realizar el diagnóstico del caso.	Realizar un diagnóstico equivocado	Falta de conocimientos necesarios	Personal		Fomentar capacitación del personal de soporte técnico.	
	4- Aplicar solución	Solución aplicada no resuelve problema	Falta de conocimientos necesarios	Personal		Fomentar capacitación del personal de	
		Imposibilidad del usuario para aplicar la solución indicada por el Soporte Técnico.	Falta de conocimientos necesarios	Personal		Soporte técnico. Fomentar Capacitación del personal de soporte técnico.	
	5- Cerrar la asistencia registrando el servicio ofrecido.	Dejar abierta la asistencia	Olvido o negligencia	Operativo		Pedir reporte periódico de asistencia donde se muestre su estatus.	

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No .	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADOS	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGACIÓN
					INTERNOS	EXTERNOS			
2	Resolver, por la vía presencial, un Problema técnico que presenta un usuario.	1- Recibir, por la vía telefónica, la solicitud del servicio técnico con la necesidad expuesta por el usuario y determina si aplica para asistencia telefónica, presencial o remota.	Imposibilidad de recibir la llamada telefónica.	Central telefónica fuera de servicio.	Operativo		Dar seguimiento al calendario de mantenimiento de la central telefónica		
		2- Registrar la Solicitud del Servicio, solicitando los datos del problema presentado por el usuario. Asigna el caso a un	Imposibilidad de realizar el registro digital	Recurso digital (PC y/o sistema de registro no disponible	Operativo		Realizar registro manualmente en el formulario Solicitud de asistencia técnica		

	soporte técnico						
	3- Realizar el diagnóstico del caso.	Realizar un diagnóstico equivocado	Falta de conocimientos necesarios	Personal		Fomentar capacitación del personal de soporte técnico.	
	4- Aplicar solución adecuada.	Solución aplicada no resuelva problema	Falta de conocimientos necesarios	Personal		Fomentar capacitación del personal de soporte técnico.	
	5- Cerrar la asistencia registrando el servicio ofrecido.	Dejar abierta la asistencia	Olvido o negligencia	Operativo		Pedir reporte periódico de asistencia donde se muestre su estatus.	

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGACIÓN
					INTERNO S	EXTERNO S			
3	Resolver un problema técnico vía conexión remota.	1- Recibir, por la vía telefónica, la solicitud del servicio técnico con la necesidad expuesta por el usuario y determina si aplica para asistencia telefónica, presencial o remota.	Imposibilidad de recibir la llamada telefónica.	Central telefónica fuera de servicio.	Operativo		Dar seguimiento al calendario de mantenimiento de la central telefónica		
		2- Registrar la Solicitud del Servicio, solicitando los datos del problema presentado por el usuario. Asigna el caso a un soporte técnico	Imposibilidad de realizar el registro digital	Recurso digital (PC y/o sistema de registro no disponible)	Operativo		Realizar registro manualmente en el formulario Solicitud de asistencia técnica		

3- Establecer la conexión remota.	Dificultad para realizar la conexión	Red lenta	Tecnológico		Mantener en buen estado los componentes de la red.		
	Imposibilidad de correr el programa de conexión remota.	Malfuncionamiento del programa de conexión remota	Tecnológico		Tener varias opciones de programas de conexión remota.		
4- Realizar el diagnóstico del caso.	Realizar un diagnóstico equivocado	Falta de conocimientos necesarios	Personal		Fomentar capacitación del personal de soporte técnico.		
5- Aplicar solución	Solución aplicada no resuelve problema	Falta de conocimientos necesarios	Personal		Fomentar capacitación del personal de soporte técnico.		
1- Cerrar la asistencia registrando el servicio ofrecido.	Dejar abierta la asistencia	Olvido o negligencia	Operativo		Pedir reporte periódico de asistencia donde se muestre su estatus.		

Institución: INSTITUTO NACIONAL DE LA VIVIENDA					Dueño del riesgo: TIC				
					Teléfono de contacto: 809-732-0600 EXT 2071				
Responsable: DIRECCIÓN DE TIC					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGA- CIÓN
					INTERNOS	EXTERNOS			
4	Resolver problema que no se resolvió vía telefónica, remota, ni en la Ubicación física. Se tuvo la necesidad de llevar el equipo al Taller de la Unidad de Soporte.	1- Registrar del reporte de avería.	Imposibilidad de realizar el registro digital	Recurso digital (PC y/o sistema de registro no disponible	Operativo		Realizar registro manualmente en el formulario Solicitud de asistencia técnica		
		2 - Trasladar el equipo al taller interno de TI.	Carrito de carga de equipos no disponible o dañado.	Falta de mantenimiento.	Operativo		Gestionar la ayuda del Depto. De mantenimiento		
		3- Diagnosticar del equipo	Realizar un diagnóstico equivocado	Falta de conocimientos necesarios	Personal		Fomentar capacitación del personal de soporte técnico.		
		4- Gestionar la compra de piezas si, si es necesario.	Tardanza en la compra de la pieza	Falta de recursos y/o expediente estancado	Económico		Gestionar la compra con tiempo y dar seguimiento.		
		5- Reparar el equipo	Equipo quede inhabilitado.	Falta de conocimientos necesarios y/o accidente y/o descuido.	Personal		Fomentar capacitación del personal de soporte técnico, incentivar la Utilización de las buenas prácticas y medidas preventivas.		

		2- Cerrar caso de avería	Dejar caso abierto	Olvido o negligencia	Operativo		Pedir reporte periódico de reparaciones donde se muestre su estatus.		
--	--	--------------------------	--------------------	----------------------	-----------	--	--	--	--

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGACIÓN
					INTERNO	EXTERNO			
5	Asegurar la disponibilidad, para su uso, de un equipo informático reportado en avería, y que no puede ser Reparado en nuestro taller interno.	1- Solicitar a la Dirección Administrativa autorización para enviar el equipo a taller externo para fines de evaluación y/o reparación.	Tardanza en la respuesta.	Expediente trasapelado.	Operativo		Dar seguimiento a la solicitud		
		2- Gestionar el envío equipo al taller externo.	Imposibilidad de trasladar el equipo al taller externo.	Vehículo de la institución no disponible.			Gestionar vehículo con tiempo, gestionar si el taller puede venir a buscar el equipo.		
		3- Recibir cotización sobre el costo de la reparación.	Tardanza en recibir la cotización.	Dedicación de tiempo insuficiente al caso por parte del taller.		Operativo	Dar seguimiento al caso hablando con los encargados del Taller a los fines de agilizar el proceso.		

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMEN TO	ACTIVIDAD ES PARA ALCANZAR LOS OBJETIVOS	POSIBLE S RIESGO S	POSIBLE S CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADOR ES	RIESGO RESIDUA L	OTRAS ACCIONE S DE MITIGA CIÓN
					INTERNO S	EXTERNO S			
6	Asegurar que los equipos y/o suministros informáticos adquiridos cumplan con las especificaciones requeridas por la Institución.	1- Realizar la verificación del o los equipos adquiridos, o procede a delegar al Soporte I, la realización de la misma - en los casos que aplique.	Que algún equipo o artículo no quede verificado.	Falta de aplicación de procedimiento de verificación.	Operativo		Incentivar al uso de procedimientos formales para la realización del proceso.		

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No .	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMEN TO	ACTIVIDAD ES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADOR ES	RIESGO RESIDUA L	OTRAS ACCION ES DE MITIGA- CIÓN
					INTERN OS	EXTERN OS			
7	Mantener el buen desempeño de los equipos informáticos (redes, computadores, impresoras, scanners, servidores, otros) que se encuentran en	1- Seleccionar equipos de acuerdo al calendario de mantenimiento de equipos.	Que se pase la fecha y no se haya seleccionado el equipo para darle mantenimiento.	Falta de seguimiento al plan.	Operativo		Incentivar a la consulta frecuente de los calendarios y planes.		
		2- Trasladar equipo al Taller de Soporte, si es necesario.	Carrito de carga de equipos no disponible o dañado.	Falta de mantenimiento.	Operativo		Gestionar la ayuda del Depto. De mantenimiento		

MATRIZ DE RIESGOS

	<p>producción</p>	<p>3- Realizar limpieza física interna y externa, utiliza herramientas de software para mantenimiento lógico del equipo (borrado de temporales, desfragmentación de disco, desinstalación de aplicaciones maliciosas, actualización de antivirus, actualización de sistema operativo, actualización de aplicaciones, etc.), formatea el equipo si es necesario y se le instalan todos los recursos de hardware y software que utiliza el usuario al que está</p>	<p>Que durante el mantenimiento se omita la aplicación de procesos que debieron aplicarse.</p>	<p>Hacer los mantenimientos de memoria.</p>	<p>Operativo</p>		<p>Utilizar checklist de verificación.</p>		
--	--------------------------	--	--	---	------------------	--	--	--	--

MATRIZ DE RIESGOS

		asignado el equipo.							
--	--	---------------------	--	--	--	--	--	--	--

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMEN TO	ACTIVIDAD ES PARA ALCANZAR LOS OBJETIVOS	POSIBLE S RIESGOS	POSIBLE S CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADOR ES	RIESGO RESIDU AL	OTRAS ACCION ES DE MITIGA CIÓN
		INTERN OS	EXTERN OS						
8	Mantener los equipos informáticos en buen estado físico y lógico, de manera que siempre están Disponibles para su uso.	1- Solicitar a Dirección Administrativa autorización para enviar el equipo a taller externo para fines de Mantenimiento Preventivo.	Tardanza en la respuesta.	Expediente extra-papelada.	Operativo		Dar seguimiento a la solicitud		
		2- Gestionar el envío equipo al taller externo.	Imposibilidad de trasladar el equipo al taller externo.	Vehículo de la institución no disponible.			Gestionar vehículo con tiempo, gestionar si el taller puede venir a buscar el equipo.		
		3- Recibir cotización sobre el costo del	Tardanza en recibir la cotización.	Dedicación de tiempo insuficiente al caso por		Operativo	Dar seguimiento al caso hablando con los		

	mantenimiento .		parte del taller.			encargados del taller a los fines de agilizar el proceso.		
	4- Solicitar autorización a la Dirección Administrativa para que el taller externo proceda a realizar el mantenimiento del equipo según cotización	Tardanza en la respuesta.	Expediente extrapapelado.	Operativo		Dar seguimiento a la solicitud		
	5- Recibir equipo con mantenimiento realizado por taller externo.	Mantenimiento no haya sido exitoso.	Falta de calificación del personal del taller		Personal	Seleccionar talleres certificados para la marca.		

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC			
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071			
					Fecha: 28/11/2019			
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL
					INTERNOS	EXTERNOS		
9	Recomendar las características que debe contener un equipo informático solicitado para que pueda insertarse con éxito en producción	1- Evaluar el requerimiento, tomando en cuenta las capacidades de hardware y software que necesita el usuario así como factores tales como tendencia tecnológica, espacio físico disponible para el equipo, estándares medioambientales y energéticos, etc.	Recomendación de Equipo con capacidad insuficiente o superior.	Falta de estudio de las necesidades de procesamiento del usuario, falta de conocimiento.	Personal		Realizar análisis de las necesidades de procesamiento, incentivar la preparación técnica.	

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGACIÓN
	O				INTERNO S	EXTERNO S			
10	Mantener control sobre los recursos informáticos y minimizar el riesgo de accesos no autorizados y pérdida de datos	1- Detectar riesgo y/o recibe reporte de brecha de seguridad y/o situación anómala.	Que el riesgo no sea detectado a tiempo.	Debilidad en el monitoreo.	Tecnológico		Constante monitoreo, y activación de alertas automáticas.		
		2- Revisar políticas de seguridad activas(Gpo's del Dominio, Firewall, Isa, Proxy, Puertos, Consola Antivirus, seguridad física y lógica, etc.)	Manejo inadecuado de las políticas de seguridad.	Falta de conocimientos, accidente.	Tecnológico		Incentivar a la actualización técnica y al uso de los protocolos para realizar todo lo relativo a seguridad.		

		3- Revisar nivel de actualización de programas (Sistemas Operativos, Aplicaciones, controladores, utilitarios, etc.)						
		4- Analizar y evaluar efecto de política de seguridad y/o actualización de software.						
		5- Crear política de seguridad nueva o modificar una existente.						
		6- Imprimir política de seguridad y/o actualización de software.	Efecto no deseado.	Aplicación directa en Ambiente de producción.			Probar las políticas de seguridad en un ambiente de prueba antes de pasarlas a producción.	

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGA- CIÓN
	INTERNOS	EXTERNOS							
11	Aprovechar los beneficios de las versiones más recientes del software base de nuestra plataforma informática al mismo tiempo que reforzamos la seguridad	4- Actualizar los repositorios de actualizaciones de productos de software instalado en los servidores, a través de actualizaciones automáticas y/o batch.	Servicio de internet fuera de servicio.	Avería, problemas en la red interna.	Tecnológico		Reportar de inmediato las averías que ocurran en el servicio de internet, monitoreo constante de la red interna.		
		Instalar las actualizaciones	Efecto no deseado.	Aplicación directa en ambiente de producción.			Probar las políticas de seguridad en un ambiente de prueba antes de pasarlas a producción.		

MATRIZ DE RIESGOS

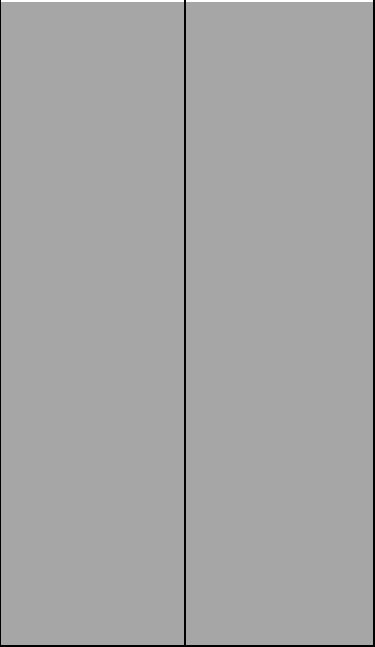
INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGA- CIÓN
					INTERNOS	EXTERNOS			
12	Minimizar el riesgo de infección por virus, programas malintencionados y spywares; los equipos de tecnología informática instalados (Servidores, Terminales, Bases de Datos, programas)	1- Actualizar componentes de la consola McAfee (motores, archivos de definición de virus, complementos, etc.) desde el site de McAfee, automáticamente o batch.	Servicio de internet fuera de servicio.	Avería, problemas en la red interna.	Tecnológico		Reportar de inmediato las averías que ocurran en el servicio de internet, monitoreo constante de la red interna.		
		2- Distribuir actualizaciones a las terminales (Automáticamente)	Terminales no reciben deploy.	Ausencia de conexión y/o agente McAfee.	Tecnológico		Aplicar actualizaciones batch en aquellos equipos que la actualización no se aplicó, monitoreo frecuente a la consola e Policy de McAfee.		

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGA- CIÓN
	INTERNOS	EXTERNOS							
13	Diseñar un sistema informático, que automatice los procesos internos y externos de los departamentos y dependencias	1- Realizar levantamiento de información sobre las necesidades y requerimientos del sistema (documentos, procesos, flujo de datos, etc)	Levantamiento incompleto.	Poca disposición de cooperación de usuarios involucrados.	Personal		Reuniones con los involucrados donde se le explique la incidencia positiva de sus aportes al producto final.		
		2- Realizar estudio de Factibilidad para la aplicación.	Análisis, Diseño, Desarrollo de software, e implementación que no cumple con las necesidades de	Falta de conocimientos	Personal		Incentivar la capacitación del personal de desarrollo de sistemas.		
		3- Diseñar la Base de Datos para la nueva aplicación.							
		4- Diseñar las Entradas, Salidas,							

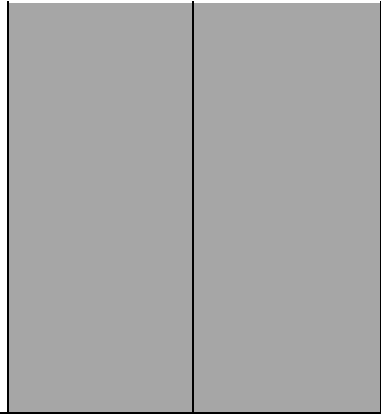
Reportes, Controles, etc.
5- Escribir los programas en el lenguaje de programación seleccionado acuerdo al Diseño realizado.
6- Prueba la aplicación con datos de prueba y datos reales.
7- Elaborar estrategia de implementación.

Procesamiento de la institución.



INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGA- CIÓN
					INTERNOS	EXTERNOS			
14	Adecuar un sistema informático existente, a los nuevos requerimientos de los departamentos de la institución	1- Realizar levantamiento de los datos necesarios para llevar a cabo las modificaciones solicitadas.	Levantamiento incompleto.	Poca disposición de cooperación de usuarios involucrados.	Personal		Reuniones con los involucrados donde se le explique la incidencia positiva de sus aportes al producto final.		
		2- Realizar estudio de Factibilidad, si es necesario.	Análisis, Diseño, Desarrollo de software, e implementación que no cumple con las necesidades de Procesamiento de la institución.	Falta de conocimientos	Personal		Incentivar la capacitación del personal de desarrollo de sistemas.		
		3- Realizar recomendaciones y/o informa sobre las implicaciones de aplicar las modificaciones solicitadas.							
4- Autorizar ejecutar los cambios solicitados.									

5- Re-Diseñar aplicación, si es necesario.
6- Modificar los programas necesarios.
7- Probar los programas ya modificados en ambiente de prueba.



MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIO NES DE MITIG A-CIÓN
	INTERNOS				EXTERNOS				
15	Asegurar la Data de la Institución de manera que se garantice la continuidad de las operaciones en caso de ocurrir una pérdida parcial o total de datos por colapso de nuestros servidores o por causas de desastre.	1- Seleccionar la data de la cual se hará backup.	Data incompleta	Omisión de la consulta a la clasificación de la data.	Operativo		Incentiva a que se consulte la clasificación de data disponible en TI donde se especifica si un tipo x de datos debe ser respaldado.		
		2- Ejecutar aplicación de backup Data Protector.	Malfuncionamiento del programa de backup	Programa desactualizado	Tecnológico		Mantener actualizado los programas.		
		3- Seleccionar las cintas para el backup	Cintas agotadas y/o dañadas.	Pedido pendiente, reutilización excedía de las cintas de backup	Operativo		Hacer pedidos con tiempo, hacer uso de las recomendaciones de reutilización del fabricante.		
		4- Arrancar la ejecución del backup.	Backup queda con errores.	Error del programa de backup	Tecnológico		Realizar prueba de integridad,		

	5- Realizar backup				ejecutar el backup de nuevo.		
	6- Depositar backup en caja de seguridad externa	Accidente de tránsito durante el traslado, mal manejo del medio magnético.	Descuido del chofer, falta de conocimiento sobre manejo de medios magnéticos.	Personal		Incentivar a la precaución durante el transporte, entrenar a los involucrados en el manejo de medios magnéticos.	

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGA- CIÓN
					INTERNOS	EXTERNOS			
16	Mantener integridad y funcionamiento óptimo de la Base de Datos	1- Ejecutar las operaciones de mantenimiento estándar (reducción de logs, reparación de tablas, índices, etc.) 3- Realizar tareas de programación, si es necesario. 4- Restaurar Base de Datos, si es necesario.	Producir daño en la base de datos	Base de datos corrompida, falta de conocimientos del personal involucrado.	Tecnológica, Personal		Realizar un backup de la Base de Datos y colocarlo en un lugar seguro antes de iniciar el mantenimiento, incentivar la capacitación del personal,		

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGA- CIÓN
					INTERNOS	EXTERNOS			
17	Asegurar que los usuarios puedan tener acceso a los recursos tecnológicos que necesitan para desempeñar las funciones que le corresponden en la institución	1- Registrar solicitud en Sistema de Administración de Documentos.	Imposibilidad de realizar el registro digital	Recurso digital (PC y/o sistema de registro no disponible	Operativo		Realizar registro manualmente en formulario de Registro de solicitud de acceso.		
		2- Determinar la pertinencia de la solicitud.	Acceso asignado no funciona de manera adecuada.	Falta de conocimientos.	Personal		Incentivar la capacitación del personal involucrado.		
		3- Realizar conexión con Servidor o Terminal, si es necesario.							
		4- Ejecutar software necesario para otorgar el acceso solicitado.							

		5- Asignar los derechos a acceso necesarios de acuerdo a la solicitud.							
--	--	--	--	--	--	--	--	--	--

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGA- CIÓN
	INTERNOS	EXTERNOS							
18	Asegurar que un usuario puede ingresar a los recursos que se encuentran disponibles en la red informática de la Institución para que posteriormente puedan ser asignados los accesos de acuerdo a las funciones que desempeña.	1- Registrar solicitud en Sistema de Administración de Documentos.	Imposibilidad de realizar el registro digital	Recurso digital (PC y/o sistema de registro no disponible	Operativo		Realizar registro manualmente en formulario de Registro de solicitud de acceso.		
		2- Determinar la pertinencia de la solicitud.	Acceso asignado no funciona de manera adecuada.	Falta de conocimientos.	Personal	Incentivar la capacitación del personal involucrado.	Riesgo Residual	Otras Acciones de Mitigación	
		3- Realizar conexión con el Servidor "Active Directory"							
		4- Ejecutar Active Directory y completa los parámetros necesarios.							

		5- Asignar el usuario a uno de los grupos definidos de la institución, si aplica.							
--	--	---	--	--	--	--	--	--	--

MATRIZ DE RIESGOS

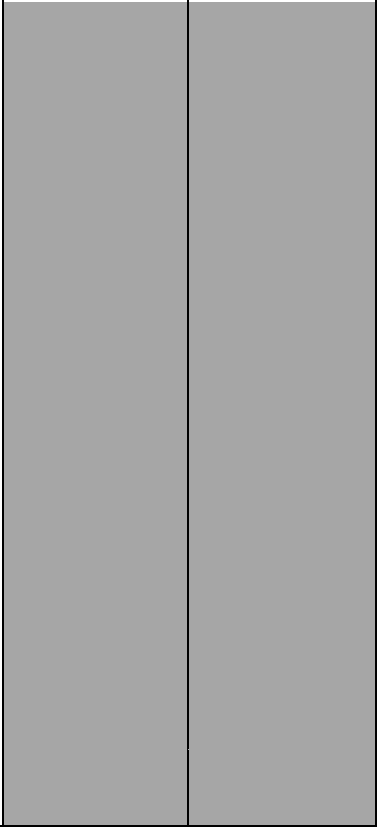
INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGA- CIÓN
					INTERNOS	EXTERNOS			
19		1- Registrar solicitud en Sistema de Administración de Documentos.	Imposibilidad de realizar el registro digital	Recurso digital (PC y/o sistema de registro no disponible	Operativo		Realizar registro manualmente en formulario de Registro de solicitud de acceso.		
	Instalar programas especiales necesarios para el buen desempeño de las actividades operativas de los sistemas y/o usuarios	2- Determinar la pertinencia de la solicitud. 3- Realizar evaluación al equipo para ver si cumple con los requisitos del programa que se desea instalar.	Imposibilidad de instalar el programa	Equipo donde se solicita la instalación no cumple con los requisitos, falta de conocimientos	Personal		Hacer uso de las buenas prácticas en la compra de equipos de manera que se proyecten las necesidades de procesamiento de las diferentes áreas, incentivar la capacitación del		

		4- Instalar programa solicitado.				personal involucrado.		
		5- Instruir al usuario sobre aspecto general de uso del programa.						

MATRIZ DE RIESGOS

INSTITUTO NACIONAL DE LA VIVIENDA (INVI)					Dueño del riesgo: TIC				
Responsable: DIRECCIÓN DE TIC					Teléfono de contacto: 809-732-0600 EXT 2071				
					Fecha: 28/11/2019				
No.	OBJETIVO/ PROCESO/ SUBPROCESO/ DEPARTAMENTO	ACTIVIDADES PARA ALCANZAR LOS OBJETIVOS	POSIBLES RIESGOS	POSIBLES CAUSAS	FACTORES A ANALIZAR		CONTROLES MITIGADORES	RIESGO RESIDUAL	OTRAS ACCIONES DE MITIGA- CIÓN
					INTERNOS	EXTERNOS			
20	Minimizar el riesgo de que un recurso informático salga de producción por un accidente, Malfuncionamiento, o sabotaje.	1- Gestionar la compra software y/o hardware necesario para monitoreo de los recursos informáticos. 2- Configurar y/o solicita la configuración a terceros de hardware y/o software de monitoreo de recursos informáticos. 3- Definir e implementa políticas que reduzcan el riesgo de un ataque o	Configuración incorrecta de parámetros para monitoreo, Inexistencia de herramientas de software para monitoreo.	Falta de previsión en el presupuesto, falta de conocimientos	Operativo, Personal		Incluir en el presupuesto partidas para herramientas de monitoreo, incentivar la Capacitación del personal involucrado.		

minimicen los efectos de una catástrofe en la plataforma tecnológica de la Institución.
4- Realizar evaluación al equipo para ver si cumple Con los requisitos del programa que se desea instalar.
5- Producir reporte periódico a partir de las herramientas de monitoreo.
6- Programar alertas.



Informes de los Riegos

Los riegos son eventualidades que no siempre se pueden evitar, pero si llegan, lo mejor es estar preparado, pues el impacto o la repercusión serán menos dañina para la institución.

No importa la clasificación del riesgo si está identificado será más fácil hacer un plan para evitar caer en él o salir del mismo si su alcance es inminente.

Cuándo nos alcanza un riesgo, afectan nuestras operaciones y directa o indirectamente nuestros activos, como son:

Nuestros servidores tanto físicos como virtuales, Nuestra data, que es uno de nuestros más grandes activos, los equipos de comunicaciones, el tiempo de repuesta de nuestros procesos, lo que nos lleva a pérdida de tiempo que es un activo intangible muy valioso y sobre todo se ven afectado nuestros clientes, proveedores y empleados que son los activos más importante, ya que de ellos dependen todo los demás y hasta la misma Data que es uno de nuestro mayores recursos

Bienes informático críticos:

En virtud de los análisis y levantamientos anteriores realizados hemos determinados que lo equipos informático imprescindibles o críticos para realizar lo que hacemos o estar en operaciones son los siguientes.

- e) los servidores principales de la red.
- f) Los medios de comunicación.
- g) El sistema contable.
- h) Estaciones telefónica, PC e Impresoras.
- i) Proveedores de servicios de internet.

Identificación de las amenaza sobre el sistema informático

Institución: INSTITUTO NACIONAL DE LA VIVIENDA				Dueño del riesgo: TI		
Dirección:				Teléfono de contacto: 809-732-0600 EXT 2071		
Fecha:				Departamento o Área: TI		
No.	RIESGOS	POSIBLES CAUSAS	IMPACTO EN LA INSTITUCION	PLAN DE REPUESTA	RECUPERACION	PRUEBA DEL PLAN
1	PERDIDA DE TODA LA DATA DE LA INSTITUCIÓN	*Por un desastre natural (Terremoto, Tormenta, Huracán) Etc. *Por un Incendio en los servidores, * Por una mala práctica de un técnico que formateo el servidor o el disco equivocado., *un ataque de un virus que llego hasta los servidores	Catastrófico debido a que se detendrían todas la operaciones de la institución.	Tener un servidor provisional, físico o virtual donde se puedan restaurar las copias de respaldo guardadas en servidores remotos para recuperar los sistemas	Evaluar los Daños de los Equipos y proceder a la reparación y/o sustitución si es necesario	

2	AVERIA EN SERVICIOS SUB CONTRATADOS	Cableado fuera de mantenimiento, ruptura de del cable o medio, conflictos en las oficinas de los proveedores	Medio	tener múltiples servicios provisionales en caso de anomalía	Darle seguimiento constante a la avería hasta su solución	
3	backup con errores o incompleto	la incidencia de un virus, sectores de disco dañado, archivos corrompidos	Alto	Hacer una prueba cada 2 semana a las copias de seguridad , montándola un una máquina virtual y comprobando la integridad de la data	Enviar la data a un centro de servicio especializado y si no se puede corregir, realizar un operativo para actualizar la data faltante y ponerla al Día	
4	Avería en la infra estructura	Accidente de una remodelación o Persona maliciosa	Alto	Hacer pruebas Periódicas simulando esa eventualidad y tener múltiple forma de reconectar con los servidores	Tener equipos para reconectar a la brevedad y la información y herramienta para hacer una BPN, en caso de que sea necesario	

5	Avería de equipo importante	Por desgaste, por antigüedad o por manos maliciosas	Alto	Hacer inventario y programas de mantenimiento preventivo, programados y con frecuencia	Tener equipos preparados con todo lo necesario que se puedan entregar en calidad de préstamo en caso de ser necesario en lo que se repara o se cambia el equipo	
---	------------------------------------	---	------	--	---	--

Procesos y/o Procedimientos.

Se define como Procedimiento al modo de proceder o el método que se implementa para llevar a cabo tareas o ejecutar determinadas acciones.

Luego de haber definido de manera detallada las políticas y los riesgos, presentamos los procedimientos establecidos en combinación de las políticas y riesgos, es decir los pasos en que se solucionan los problemas en el área de TIC.

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.			Fecha: 28 /11/2019	
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
			(Si / No)				Intermedios	Finales
1	ASISTENCIA TÉCNICA VIA TELEFONICA	1- Recepción y Registro de Solicitud de Asistencia Telefónica	Si	Resolver, por la vía telefónica, un Problema técnico que presenta un usuario.	Soporte Técnico	1- Recibe, por la vía telefónica, la solicitud del servicio técnico con la necesidad expuesta por el usuario y determina si aplica para asistencia telefónica, presencial o remota.		ASISTENCIA TECNICA TELEFONICA REALIZADA
						2- Registra la Solicitud del Servicio, solicitando los datos del problema presentado por el usuario. Asigna el caso a un soporte técnico		
		2- Evaluación, Diagnóstico, y Solución, vía Telefónica, de Problemas de Soporte Técnico de TI presentados por un Usuario	Si		Soporte Técnico	1- Analiza el problema presentado por el usuario del servicio de TI.		
		2- Realiza el diagnóstico del caso.						
				Soporte Técnico	3- Determina las acciones necesarias para la solución del problema planteado.			
					4- Instruye al usuario para que aplique las acciones necesarias para resolver el problema planteado.			
				Dir. de TIC	5- Verifica con el usuario que el problema fue resuelto e informa al Encargado de TI.			
					6- Transfiere el problema - si es necesario - al Encargado de TI.			
		4- Supervisión y Cierre de Asistencia	Si		Dir. de TIC	1- Supervisa que el problema presentado haya sido resuelto		
					Soporte Técnico	2- Cierra la asistencia registrando el servicio ofrecido.		

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional..			Fecha: 28 /11/2019	
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
			(Si / No)				Intermedios	Finales
2	ASISTENCIA TÉCNICA PRESENCIAL	1- Recepción y Registro de Solicitud de Asistencia Presencial	Si	Resolver, por la vía presencial, un Problema técnico que presenta un usuario.	Soporte Técnico	1- Recibe, por la vía telefónica, la solicitud del servicio técnico con la necesidad expuesta por el usuario y determina si aplica para asistencia telefónica, presencial o remota. 2- Registra la Solicitud del Servicio, solicitando los datos del problema presentado por el usuario. Asigna el caso a un soporte técnico		ASISTENCIA TECNICA PRESENCIAL REALIZADA
		2- Evaluación, Diagnóstico, y Solución, vía Presencial, de Problemas de Soporte Técnico de TI presentados por un Usuario	Si		Soporte Técnico	1- Analiza el problema presentado por el usuario del servicio de TI. 2- Realiza el diagnóstico del caso. 3- Determina las acciones necesarias para la solución del problema planteado y las aplica.		
					Soporte Técnico	4- Transfiere el problema - si es necesario - al Encargado de TI. 5- Verifica con el usuario que el problema fue resuelto e informa al Encargado de TI.		
4- Supervisión y Cierre de Asistencia	Si	Dir. de TIC	1- Supervisa que el problema presentado haya sido resuelto					
				Soporte Técnico	2- Cierra la asistencia registrando el servicio ofrecido.			

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda			Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.			Fecha: 28 /11/2019		
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado (Si / No)	Objetivo del Proceso	Responsable (Dueño del)	Descripción del Proceso	Productos	
							Intermedios	Finales
3	ASISTENCIA TÉCNICA DADA (CONEXIÓN REMOTA) (HELP DESK).	1- Recepción y Registro de Solicitud de Asistencia Remota	SI	Resolver un problema técnico vía conexión remota.	Soporte Técnico	1- Recibe, por la vía telefónica, la solicitud del servicio técnico con la necesidad expuesta por el usuario y determina si aplica para asistencia telefónica, presencial o remota.		ASISTENCIA TÉCNICA REMOTA REALIZADA
						2- Registra la Solicitud del Servicio, solicitando los datos del problema presentado por el usuario. Asigna el caso a un soporte técnico		
		2- Evaluación, Diagnóstico, y Solución, vía Remota, de Problemas de Soporte Técnico de TI presentados por un Usuario	SI	Resolver un problema técnico vía conexión remota.	Dir. de TIC	1- Analiza el problema presentado por el usuario del servicio de TI.		
		2- Realiza el diagnóstico del caso.						
		3- Determina las acciones necesarias para la solución del problema planteado y las aplica.						
				4- Transfiere el problema a Soporte I, si es necesario.				
				5- Verifica con el usuario que el problema fue resuelto y solicita a Soporte I el cierre del caso.				
				6- Transfiere el problema a Soporte I, si es necesario.				
		3- Cierre de Asistencia	SI		Soporte Técnico	1- Cierra la asistencia registrando el servicio ofrecido.		

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda			Dirección:			Fecha: 28 /11/2019		
Dirección de Tecnología de la Información y la Comunicación			Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.					
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado (Si / No)	Objetivo del Proceso	Responsable (Dueño del)	Descripción del Proceso	Productos	
							Intermedios	Finales
4	REPARACIÓN INTERNA DE EQUIPOS INFORMATICOS	1- Recepción y Registro de Reporte de Avería en Equipo Informático.	Si	Resolver problema que no se resolvió vía telefónica, remota, ni en la ubicación física. Se tuvo la necesidad de llevar el equipo al taller de la Unidad de Soporte.	Soporte Técnico	1 - Recibe el reporte de avería del equipo informático, por parte del usuario.		
						2- Registra del reporte de avería.		
		2- Evaluación, Diagnóstico, y Solución Interna de Avería en Equipo Informático.	Si		Soporte Técnico	2 - Traslada el equipo al taller interno de TI.		
					Dir. de TIC	4- Transferir a proceso de reparación de avería en taller externo, si es necesario.		
						5 - Solicita piezas al Dir. de TIC, si es necesario.		
					Soporte Técnico	6- Solicita piezas existentes al almacén, y/o Gestiona las compras de otras, si es necesario.		
						7- Instala piezas		
					Dir. de TIC	8- Prueba el equipo, verificando que el mismo esté funcione correctamente e informa al Encargado de TI		
						1- Supervisa que la avería haya resuelta.		
		Soporte Técnico	1- Entrega el equipo reparado al usuario.					
	Supervisión y Cierre de avería		2- Cierra caso de avería					
								REPARACIÓN INTERNA DE EQUIPOS INFORMATICOS REALIZADA

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito		Fecha: 28 /11/2019			
Dirección de Tecnología de la Información y la Comunicación									
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado (Si / No)	Objetivo del Proceso	Responsable (Dueño del)	Descripción del Proceso		Productos	
						Intermedios	Finales		
5	REPARACIÓN EXTERNA DE EQUIPO INFORMATICO	1- Evaluación interna y envió a taller externo	Si	Asegurar la disponibilidad, para su uso, de un equipo informático reportado en avería, y que no Puede ser reparado en nuestro taller interno.	Dir. de TIC	1 - Recibe reporte de evaluación de Equipo de la Unidad de Soporte indicando que no se puede reparar el equipo en el taller interno.			
						2- Solicita a la Dirección Administrativa autorización para enviar el equipo a taller externo para fines de evaluación y/o reparación.			
						3- Recibe autorización aprobada y Gestiona la salida del mismo hacia taller externo.			
					Soporte Técnico	4- Actualiza el registro de la avería haciendo constar que será reparado en taller externo.			
		Dir. de TIC	5- Gestiona el envío equipo al taller externo.						
			1- Recibe cotización sobre el costo de la reparación.						
			2- Determina factibilidad de la reparación.						
			3 Solicita autorización a la Dirección Administrativa para que el taller externo proceda a reparar el equipo según cotización						
		2- Análisis de propuesta de reparación externa.	Si			4- Recibe aprobación de reparación.			

REPARACIÓN EXTERNA DE EQUIPOS INFORMATICOS REALIZADA

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito		Fecha: 28 /11/2019			
Dirección de Tecnología de la Información y la Comunicación									
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado (Si / No)	Objetivo del Proceso	Responsable (Dueño del)	Descripción del Proceso		Productos	
						Intermedios	Finales		
Cont. 5	REPARACIÓN EXTERNA DE EQUIPO INFORMATICO	3- Supervisión y Cierre de avería		Asegurar la disponibilidad, para su uso, de un equipo informático reportado en avería, y que no Puede ser reparado en nuestro taller interno.	Soporte Técnico	1- Recibe equipo reparado		REPARACIÓN EXTERNA DE EQUIPOS INFORMATICOS REALIZADA	
						2- Prueba el equipo, verificando que el mismo esté funcione correctamente e informa al Encargado de TI			
						3- Supervisa que la avería haya resuelta.			
						4- Entrega el equipo reparado al usuario.			
						5- Cierra caso de avería			

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda			Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esmerilla, Santo Domingo, Distrito		Fecha: 28 /11/2019			
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado	Objetivo del Proceso	Responsable (Dueño del)	Descripción del Proceso	Productos	
			(Si / No)			Intermedios	Finales	
6	VERIFICACION DE EQUIPOS Y/O SUMINISTROS INFORMATICOS ADQUIRIDOS	1- Verificación de Equipos y/o Suministros Adquiridos Informáticos	SI	Asegurar que los equipos y/o suministros informáticos adquiridos cumplan con las especificaciones Requeridas por la Institución.	Dir. de TIC	<p>1- Recibe la solicitud de verificación de equipos y/o suministros informáticos adquiridos.</p> <p>2- Realiza la verificación del o los equipos adquiridos, o procede a delegar al Soporte I, la realización de la misma - en los casos que aplique.</p> <p>3- Firma el conduce de los equipos recibidos, conjuntamente con: un representante de la Gerencia de Revisión y Análisis, un representante de la Contraloría y el Encargado de Suministro.</p> <p>4- Remite informe al Departamento de Compras, sobre la verificación realizada.</p>		EQUIPOS / SUMINISTROS INFORMATICOS ADQUIRIDOS VERIFICADOS

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.		Fecha: 28 /11/2019				
Dirección de Tecnología de la Información y la Comunicación										
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos			
			(Si / No)				Intermedios	Finales		
7	EJECUCION DE MANTENIMIENTO PREVENTIVO INTERNO	1 - Recepción/preparación de equipo para mantenimiento preventivo.	SI	Mantener el buen desempeño de los equipos informáticos (redes, computadores, impresoras, scanners, servidores, otros) que se encuentran en producción	Soporte Técnico	1- Selecciona equipos para dar mantenimiento		MANTENIMIENTO PREVENTIVO INTERNO REALIZADO		
						2- Trasladar equipo al Taller de Soporte, si es necesario.				
						3- Registrar entrada a Taller, si es necesario.				
						4- Asignar mantenimiento a técnico				
					2- Realización y Verificación de Mantenimiento Preventivo	SI			Soporte Técnico	1- Realiza limpieza física interna y externa, utiliza herramientas de software para mantenimiento lógico del equipo (borrado de temporales, desfragmentación de disco, desinstalación de aplicaciones maliciosas, actualización de antivirus, actualización de sistema operativo, actualización de aplicaciones, etc.), formatea el equipo si es necesario y se le instalan todos los recursos de hardware y software que utiliza el usuario al que está asignado el equipo.
										2- Verifica todas las operaciones del mantenimiento con checklist de mantenimiento estándar.
		3- Instalación del equipo en su ubicación de origen.								
		3- Supervisión y Cierre	SI	Dir. de TIC	1- Supervisa el cumplimiento del calendario de mantenimiento preventivo.					
				Soporte Técnico	Asistencia Cerrada					

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito		Fecha: 28 /11/2019			
Dirección de Tecnología de la Información y la Comunicación									
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado (Si / No)	Objetivo del Proceso	Responsable (Dueño del)	Descripción del Proceso		Productos	
						Intermedios	Finales		
8	MANTENIMIENTO EXTERNO PREVENTIVO	1- Evaluación interna y envió a taller externo	Si	Mantener los equipos informáticos en buen estado físico y lógico, de manera que siempre están disponibles para su uso.	Dir. de TIC	1 - Recibe reporte de evaluación de Equipo de la Unidad de Soporte indicando que no contamos con los recursos para realizar el mantenimiento del equipo en nuestro taller interno.			MANTENIMIENTO EXTERNO PREVENTIVO REALIZADO
						2- Solicita a la Dirección Administrativa autorización para enviar el equipo a taller externo para fines de Mantenimiento Preventivo.			
						3- Recibe autorización aprobada y Gestiona la salida del mismo hacia taller externo.			
						4- Actualiza el registro del mantenimiento haciendo constar que será realizado en taller externo.			
		2- Análisis de propuesta de reparación externa.	Si		Dir. de TIC	5- Gestiona el envío equipo al taller externo.			
						1- Recibe cotización sobre el costo del mantenimiento.			
						2- Determina factibilidad del mantenimiento.			
						3 Solicita autorización a la Dirección Administrativa para que el taller externo proceda a realizar el mantenimiento del equipo según cotización			
						4- Recibe aprobación de mantenimiento preventivo externo.			

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito			Fecha: 28 /11/2019	
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado (Si / No)	Objetivo del Proceso	Responsable (Dueño del)	Descripción del Proceso	Productos	
							Intermedios	Finales
Cont. 8	MANTENIMIENTO EXTERNO PREVENTIVO	3- Supervisión y Cierre de avería		Asegurar la disponibilidad, para su uso, de un equipo informático reportado en avería, y que no puede ser reparado en nuestro taller interno.	Soporte Técnico	1- Recibe equipo con mantenimiento realizado por taller externo.		MANTENIMIENTO EXTERNO PREVENTIVO REALIZADO
						2- Prueba el equipo, verificando que el mismo esté funcione correctamente e informa al Encargado de TI		
						3- Actualiza ficha del equipo		
					Dir. de TIC	4- Supervisa que el mantenimiento haya sido realizado.		
					Soporte Técnico	4- Entrega el equipo al usuario.		
5- Cierra caso de avería								

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda			Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.			Fecha: 28 /11/2019		
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
			(Si / No)				Intermedios	Finales
9	RECOMENDACION PARA COMPRA DE EQUIPOS INFORMATICOS	1 - Solicitud de equipo recibida informalmente.	SI	Recomendar las características que debe contener un equipo informático solicitado para que pueda insertarse con éxito en producción	Dir. de TIC	1- Recibe Solicitud de recomendación técnica para compra equipo desde la Dirección Administrativa. 2- Evalúa el requerimiento, tomando en cuenta las capacidades de hardware y software que necesita el usuario así como factores tales como tendencia tecnológica, espacio físico disponible para el equipo, estándares medioambientales y energéticos, etc. 3- Remite a la Dirección Administrativa la recomendación técnica de lugar.		RECOMENDACION PARA COMPRA DE EQUIPOS INFORMATICOS REALIZADA

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.			Fecha: 28 /11/2019	
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
			(Si / No)				Intermedios	Finales
10	IMPLEMENTACION DE MEDIDA DE SEGURIDAD	1- Monitoreo de plataforma de seguridad	Si	Mantener control sobre los recursos informáticos y minimizar el riesgo de accesos no autorizados y perdida de datos	Enc. de TI Soporte Técnico.	1- Detecta riesgo y/o recibe reporte de brecha de seguridad y/o situación anómala.		POLITICA DE SEGURIDAD Y/O ACTUALIZACION DE SOFTWARE IMPLEMENTADA
						2- Revisar políticas de seguridad activas (Gpo's del Dominio, Firewall, Isa, Proxy, Puertos, Consola Antivirus, seguridad física y lógica, etc.)		
						3- Revisar nivel de actualización de programas (Sistemas Operativos, aplicaciones, controladores, utilitarios, etc.)		
						4- Analiza y evalúa efecto de política de seguridad y/o actualización de software.		
						4- Crea política de seguridad nueva o modificar una existente.		
						5- Autoriza aplicación seguridad.		
						6- Prueba política de seguridad y/o actualización de software en ambiente de prueba.		
		2- Evaluación, Prueba y Puesta en marcha de política de seguridad y/o actualización de software.	Si		Dir. de TIC	7- Implementar política de seguridad y/o actualización de software en ambiente de producción.		

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.			Fecha: 28 /11/2019	
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
			(Si / No)				Intermedios	Finales
	ACTUALIZACION SOFTWARE DE SISTEMAS (PLATAFORMA Y OTROS)	1 - Captación de actualización de software.	Si	Aprovechar los beneficios de las versiones más recientes del software base de nuestra plataforma informática al mismo tiempo que reforzamos la seguridad	Dir. de TIC	1- Consulta portales de internet de los fabricantes de Software instalados en la plataforma tecnológica de la Institución (Sistemas Operativos, Antivirus, Aplicaciones, Driver, Utilitarios, etc.) instalados en la plataforma tecnológica de la Institución.		ACTUALIZACION SOFTWARE DE SISTEMAS (PLATAFORMA Y OTROS) REALIZADA
						2- Recibe boletines y/o correo electrónico sobre aviso de nuevas versiones de software.		
						3- Consulta con los representantes de Software de los programas instalados en la plataforma tecnológica de la Institución.		
						4- Actualiza los repositorios de actualizaciones de productos de software instalado en los servidores, a través de actualizaciones automáticas y/o batch.		
		2- Prueba de Actualizaciones	Si		Soporte Técnico	Instala, comprueba funcionamiento de las actualizaciones en ambiente de prueba.		
						Genera reporte recomendando la instalación o no de la actualización en ambiente de producción.		
Cont. 11	ACTUALIZACION SOFTWARE DE SISTEMAS (PLATAFORMA Y OTROS)	3 - Implementación de Actualizaciones	Si	Aprovechar los beneficios de las versiones más recientes del software base de nuestra plataforma informática al mismo tiempo que reforzamos la seguridad	Soporte Técnico	Desinstala actualizaciones de ambiente de prueba y documenta los datos de la misma.		ACTUALIZACION SOFTWARE DE SISTEMAS (PLATAFORMA Y OTROS) REALIZADA
					Dir. de TIC	Instala las actualizaciones en Servidores en Producción, si es necesario.		
						Instala y/o distribuye (Deploy) las actualizaciones en los terminales conectados a la red de datos de la Institución, si es necesario.		
						Actualiza documentación sobre actualizaciones.		

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda			Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.			Fecha: 28 /11/2019		
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
			(Si / No)				Intermedios	Finales
12	ACTUALIZACION DE CONSOLA EPOLICY DE LA SUITE MCAFEE	1- Obtención actualizaciones para la Consola e Policy . McAfee	SI	Minimizar el riesgo de infección por virus, programas malintencionados y spywares; los equipos de tecnología informática instalados (Servidores, Terminales, Bases de Datos, programas)	Dir. de TIC	1- Conecta al site de McAfee (automáticamente, o por petición)		CONSOLA EPOLICY DE LA SUITE MCAFEE ACTUALIZADA
						2- Actualiza componentes de la consola McAfee (motores, archivos de definición de virus, complementos, etc.)		
		2- Deploy a terminales	SI		Dir. de TIC	1- Distribuye actualizaciones a las terminales (Automáticamente)		
						3- Aplica actualizaciones batch en aquellos equipos que la actualización no se aplicó.		
						2- Verifica que la actualización se aplique a todos los equipos.		
						3- Actualiza registro de control de actualizaciones de software.		

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.			Fecha: 28 /11/2019	
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado (Si / No)	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
							Intermedios	Finales
13	DISEÑO DE SOFTWARE (APLICACIONES)	1- Recepción y Registro de solicitud de Desarrollo de Aplicación o Programa Informático.	Si	Diseñar un sistema informático, que automatice los procesos internos y externos de los departamentos y dependencias	Secretaria	1- Recibe solicitud con requerimientos de la nueva aplicación desde el departamento solicitante.		DISEÑO DE SOFTWARE (APLICACIONES) IMPLEMENTADA
		2 - Análisis preliminar y detallado	Si		Dir. de TIC	2- Registra la solicitud en el portafolio de aplicaciones pendiente de estudio y desarrollo.		
					Dir. de TIC	1- Autoriza el estudio para el Análisis de la aplicación solicitada.		
		3- Diseño de la nueva aplicación	Si		Programador, Dir. de TIC	2- Realiza levantamiento de información sobre las necesidades y requerimientos del sistema (documentos, procesos, flujo de datos, etc)		
					Programador, Dir. de TIC	3- Realiza estudio de Factibilidad para la aplicación.		
					Programador, Dir. de TIC	4- Realiza recomendaciones para Diseño de la nueva aplicación.		
		4- Desarrollo del software de la nueva aplicación.	Si		Programador	Diseña la Base de Datos para la nueva aplicación.		
Diseña las Entradas, Salidas, Reportes, Controles, etc.								
Cont. 13	DISEÑO DE SOFTWARE (APLICACIONES)	5- Prueba e Implementación de la nueva aplicación.	Si		Dir. de TIC	1- Elabora estrategia de implementación.		DISEÑO DE SOFTWARE (APLICACIONES) IMPLEMENTADA
					Dir. de TIC	2- Autoriza la instalación de la aplicación a los usuarios que la utilizarán.		
					Soporte Técnico	3- Instala la aplicación autorizada.		
					Programador	4- Entrena a los usuarios de la nueva aplicación en el uso de la misma.		
					Dir. de TIC	5- Supervisa todas las etapas del proceso.		

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.			Fecha: 28 /11/2019	
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
			(Si / No)				Intermedios	Finales
14	MODIFICACION SOFTWARE (APLICACIONES)	1- Recepción y Registro de solicitud de Modificación de Aplicación o Programa Informático.	Si	Adecuar un sistema informático existente, a los nuevos requerimientos de los departamentos de la institución	Secretaria	1- Recibe solicitud para agregar, modificar, eliminar, o rediseñar alguna funcionalidad de una aplicación existente.		MODIFICACION SOFTWARE (APLICACIONES) IMPLEMENTADA
					Dir. de TIC	2- Registra la solicitud en el portafolio de aplicaciones pendiente de modificación.		
					Dir. de TIC	1- Autoriza el estudio para el Análisis de los cambios solicitados para la aplicación.		
					Programador, Enc. de TI	2- Realiza levantamiento de los datos necesarios para llevar a cabo las modificaciones solicitadas.		
					Programador, Enc. de TI	3- Realiza estudio de Factibilidad, si es necesario.		
					Programador	4- Realiza recomendaciones y/o informa sobre las implicaciones de aplicar las modificaciones solicitadas.		
					Dir. de TIC	5- Autoriza ejecutar los cambios solicitados.		
		3- Re-Diseño de aplicación	Si		Programador	Re-Diseña aplicación, si es necesario.		
		4- Modificación de programa existente.	Si		Programador	Modifica los programas necesarios. Prueba los programas ya modificados en ambiente de prueba.		
Cont. 14	MODIFICACION SOFTWARE (APLICACIONES)	5- Prueba e Implementación de cambios en aplicación existente.	Si	Adecuar un sistema informático existente, a los nuevos requerimientos de los departamentos de la institución	Dir. de TIC	Autoriza la instalación del ejecutable actualizado de la aplicación modificada.		MODIFICACION SOFTWARE (APLICACIONES) IMPLEMENTADA

				Programador	Actualiza el registro de Control de Versiones para aplicaciones.		
				Soporte Técnico	Instala ejecutable actualizado autorizado.		
				Programador	4- Entrena a los usuarios de la nueva aplicación en el uso de la misma.		
				Dir. de TIC	5- Supervisa todas las etapas del proceso.		

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda			Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.			Fecha: 28 /11/2019				
Dirección de Tecnología de la Información y la Comunicación										
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos			
			(Si / No)				Intermedios	Finales		
15	RESGUARDO DE LA DATA DE LA INSTITUCION	1- Definición del Ámbito del Backup.	Si	Asegurar la Data de la Institución de manera que se garantice la continuidad de las operaciones en caso de ocurrir una pérdida parcial o total de datos por colapso de nuestros servidores o por causas de desastre.	Dir. de TIC	1- Determina data a la cual se le hará backup.		RESGUARDO DE LA DATA DE LA INSTITUCION REALIZADO		
		2- Creación del Backup	Si			2- Ejecuta aplicación de backup Data Protector.				
						3- Configurar el programa Data Protector con las opciones adecuadas para hacer el backup de los datos requeridos.				
3- Verificación, Traslado y resguardo de Backup	Si	1- Escanea las cintas de backup en las cuales se hará el mismo.								
		2- Inicializa las cintas de backup y las asigna a un Media Pool.								
		3- Selecciona el tipo de backup a realizar de acuerdo a la política predefinida.								
		4- Arranca la ejecución del backup, o lo deja programado para que se ejecute en la fecha y hora establecida.								
						1- Verifica que el backup se realizó correctamente. Hace revisión de integridad.				
						2- Seleccionar las cintas de backup a trasladar a la caja fuerte.				
						3- Depositar cintas en caja fuerte				
						4- Actualizar Registro de Cintas de Backup Depositadas en Caja Fuerte Externa.				

Institución: Instituto Nacional de la Vivienda				Dirección:		Fecha: 28 /11/2019		
Dirección de Tecnología de la Información y la Comunicación				Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.				
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
			(Si / No)				Intermedios	Finales
16	MANTENIMIENTO DE BASE DE DATOS	1- Mantenimiento de la Base de Datos de la Institución	Si	Mantener integridad y funcionamiento óptimo de la Base de Datos	Dir. de TIC	1- Consulta calendario de mantenimientos y da seguimiento al mismo.		MANTENIMIENTO DE BASE DE DATOS REALIZADO
						2- Recibe reporte de error en uno de los sistemas conectados a la base de datos de la Institución.		
					Programador	3- Realiza backup de la Base de Datos.		
						4- Ejecuta las operaciones de mantenimiento estándar (reducción de logs, reparación de tablas, índices, recomposición de data corrompida)		
						5- Realiza tareas de programación, si es necesario.		
					Dir. de TIC	5- Restaura Base de Datos, si es necesario.		
6- Supervisa la realización de los procesos de mantenimiento.								

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.		Fecha: 28 /11/2019		
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado (Si / No)	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
							Intermedios	Finales
17	ASIGNACION DE ACCESO A RECURSO INFORMATICO	1- Recepción y Registro de Solicitud	SI	Asegurar que los usuarios puedan tener acceso a los recursos tecnológicos que necesitan para desempeñar las funciones que le corresponden en la institución	Secretaria	1- Recibe comunicación de solicitud de acceso a recurso informático.		ACCESO A RECURSO INFORMATICO ASIGNADO
		2- Asignación de Acceso a Recurso Informático.	SI			2- Registra solicitud en Sistema de Administración de Documentos.		
						3- Determina la pertinencia de la solicitud.		
						4- Realiza conexión con Servidor o Terminal, si es necesario.		
						5- Ejecuta software necesario para otorgar el acceso solicitado.		
					Dir. de TIC	6- Asigna los derechos a acceso necesarios de acuerdo a la solicitud.		
						7- Actualiza registro de Acceso a Recursos Informáticos.		
						8- Informa al solicitante, y requiere firma de documento en la que el usuario se responsabiliza por los eventos que ocurran a su nombre en el recurso al que se le ha otorgado acceso.		

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.		Fecha: 28 /11/2019		
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado (Si / No)	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
							Intermedios	Finales
19	INSTALACION DE PROGRAMA INFORMATICO	1- Instalación de programa informático	SI	Instalar programas especiales necesarios para el buen desempeño de las actividades operativas de los sistemas y/o usuarios	Secretaria	1- Recibe comunicación solicitando la instalación de un programa o aplicación ausente en el equipo del solicitante. 2- Registra solicitud en Sistema de Administración de Documentos.		PROGRAMA INFORMATICO INSTALADO
					Dir. de TIC	3- Determina la pertinencia de la solicitud.		
					Soporte I	4- Realiza evaluación al equipo para ver si cumple con los requisitos del programa que se desea instalar.		
						5- Instala programa solicitado.		
						6- Instruye al usuario sobre aspectos generales de uso del programa.		
						8- Informa al Enc. De TIC.		
					Dir. de TIC	9- Actualiza registro de Usuarios de Programas.		

Matriz de Procesos

Institución: Instituto Nacional de la Vivienda				Dirección: Ave. Pedro Henríquez Ureña esq. Alma Mater, La Esperilla, Santo Domingo, Distrito Nacional.		Fecha: 28 /11/2019		
Dirección de Tecnología de la Información y la Comunicación								
No.	Nombre del Proceso	Subprocesos / Micro proceso	Documentado (Si / No)	Objetivo del Proceso	Responsable (Dueño del proceso)	Descripción del Proceso	Productos	
							Intermedios	Finales
20	MONITOREO DE PLATAFORMA TECNOLÓGICA	1- Instalación de programa informático	SI	Minimizar el riesgo de que un recurso informático salga de Producción por un accidente, malfuncionamiento, o sabotaje.	Dir. de TIC	1- Gestiona la compra software y/o hardware necesario para monitoreo de los recursos informáticos. 2- Configura y/o solicita la configuración a terceros de hardware y/o software de monitoreo de recursos informáticos. 3- Define e implementa políticas que reduzcan el riesgo de un ataque o minimicen los efectos de una catástrofe en la plataforma tecnológica de la Institución. 4- Realiza evaluación al equipo para ver si cumple con los requisitos del programa que se desea instalar. 5- Produce reporte periódicos a partir de las herramientas de monitoreo. 6- Programa alertas. 7- Informa a Usuarios y Autoridades de la Institución sobre la ocurrencia de eventos importantes detectados. 8- Registra los eventos para fines actualizar fuente de conocimientos previos y para fines estadísticos.		MONITOREO DE PLATAFORMA TECNOLÓGICA REALIZADA

Instituto Nacional de la Vivienda (**INVI**)

Creado por: Dirección de Tecnología (**TIC**)

Elaborada bajo los lineamientos de la ISO 27000, Metodología PSI Y SGSI, para la creación del Manual de Seguridad y políticas de Tecnología de la Información y Comunicación.