UNIDAD DE INVESTIGACIONES FINANCIERAS

UIF

POLITICAS DE SEGURIDAD DE LA INFORMACION (PSI)

Unidad de Investigaciones Financieras
Vo.Bo.
C.L.B.
JSTI

La Paz, Octubre de 2014

Unidad de Investigaciones Financieras
Vo.Bo.
J.L.C.G.
JSTI

Unidad de Investigaciones Financieras
Estado Plurinacional de Bolivia

La Paz, 11 de Junio de 2015
RESOLUCIÓN ADMINISTRATIVA N° UIF/045/2015

VISTOS:

El INFORME UIF/SIS/33201/2014 de 23 de octubre de 2014, suscrito por el Jefe de Sistemas y Tecnologías de la Información, mediante el cual se solicita la emisión de Resolución Administrativa que apruebe las Políticas de Seguridad de la Información"; y la instrucción de la Máxima Autoridad Ejecutiva de la institución mediante Nota de COMUNICACIÓN UIF/DIR/34628/2014 y demás antecedentes.

CONSIDERANDO:

Que, la Constitución Política del Estado Plurinacional, en su artículo 232, dispone: "*La Administración Pública se rige por los principios de legitimidad, legalidad, imparcialidad, publicidad, compromiso e interés social, ética, transparencia, igualdad, competencia, eficiencia, calidad, honestidad, responsabilidad y resultados*"; de la misma forma, el articulo 235, en su numeral 2, determina que las servidoras y servidores públicos, tienen la obligación de: "*Cumplir sus responsabilidades, de acuerdo con los principios de la función pública*".

Que, el numeral 44 del artículo 2 de la Ley N° 1768, de modificaciones al Código Penal, de 10 de marzo de 1997, establece la inclusión del artículo 185 ter., por la cual se crea la Unidad de Investigaciones Financieras como parte de la estructura orgánica de la Superintendencia de Bancos y Entidades Financieras, ahora Autoridad de Supervisión del Sistema Financiero, cuya organización y atribuciones se encuentran establecidas en el D.S. N° 24771 Reglamento de la Unidad de Investigaciones Financieras.

Que, el artículo 495 del Capítulo III de la Ley 393 de fecha 05 de agosto de 2013, establece que: "La Unidad de Investigaciones Financieras - *UIF, es una entidad descentralizada, con autonomía de gestión administrativa, financiera, legal y técnica, bajo tuición del Ministerio de Economía y Finanzas Públicas, encargada de normar el régimen de lucha contra el lavado de dinero y financiamiento del terrorismo en consulta con el Ministerio de Economía y Finanzas Públicas y las autoridades de supervisión; investigar los casos en los que se presuma la comisión de delitos de legitimación de ganancias ilícitas, financiamiento al terrorismo y otros de su competencia; y realizar el análisis, tratamiento y transmisión de información para prevenir y detectar los delitos señalados en el presente Artículo*".

Que, el parágrafo I y II del Articulo 498 de la citada ley, establece que la Máxima Autoridad Ejecutiva de la UIF es la Directora o Director General Ejecutivo, que será designado mediante Resolución Suprema, el mismo que define los asuntos de competencia de la UIF a través de Resoluciones Administrativas.

Calle Loayza N° 155 ■ Teléfono/Fax (591-2) 2188988 ■ Teléfono: (591-2) 2313077
PO BOX N° 7915 ■ Página web: www.uif.gob.bo ■ Correo electrónico: info@uif.gob.bo
La Paz - Bolivia

Que, el Decreto Supremo N° 1969 de 9 de abril de 2014 reglamenta la transformación de la Unidad de Investigaciones Financieras de órgano desconcentrado de la Autoridad de Supervisión del Sistema Financiero ASFI a Entidad Publica Descentralizada bajo tuición del Ministerio de Economía y Finanzas Públicas MEFP.

Que, mediante Ley N° 4072, de 27 de julio de 2009, aprueba el Memorándum de Entendimiento entre los Gobiernos de los Estados del Grupo de Acción Financiera de Sudamérica contra el Lavado de Activos (GAFISUD), donde Bolivia como Estado miembro se compromete a cumplir con los Estándares Internacionales sobre el Enfrentamiento al Lavado de Dinero, el Financiamiento del Terrorismo y la Proliferación al respecto en cumplimiento a la Recomendación 29 en su inciso D.- Seguridad y Confidencialidad de la Información, establece que: *"La información recibida, procesada, conformada difundida por la UIF debe estar firmemente protegida, podrá intercambiarse utilizarse solamente de acuerdo con los procedimientos convenidos, las políticas leyes reglamentos aplicables. La UIF debe, por tanto, disponer de reglas que rigen la seguridad confidencialidad de dicha información, incluyendo procedimientos para el manejo, almacenamiento, difusión protección de tal información, así como para el acceso la misma. La UIF debe asegurarse de que sus funcionarios cuenten con los niveles de autorización necesarios en cuanto la seguridad, la comprensión de sus responsabilidades en el manejo difusión de información delicada confidencial. La UIF debe asegurarse de que existe un acceso limitado sus instalaciones la información, incluyendo sistemas de tecnología de la información".*

CONSIDERANDO:

Que, el informe UIF/SIS/33201/2014 de 23 de octubre de 2014, emitido por el Jefe de Sistemas y Tecnologías de la Información, indica que "*...se ve la imperiosa necesidad de contar con Políticas de Seguridad Informática, las cuales permitirán garantizar la confidencialidad, integridad, disponibilidad de los datos y adicionalmente, control, autenticidad y utilidad de lo referente a Tecnologías de la Información, política que además de ser una norma será una herramienta organizacional para concientizar a todos los funcionarios de la UIF sobre la importancia y sensibilidad de la Información y servicios críticos que permiten a la entidad crecer y mantenerse posesionada, por lo que se recomienda emitir el correspondiente informe Legal y posterior emisión de la Resolución correspondiente aprobando documento Políticas de Seguridad de la Información de la UIF*".

Que, el INFORME/UIF/DAFL/JAL/303/2015 de 11 de junio de 2015, concluye que, en mérito a la transformación de la Unidad de Investigaciones Financieras, de entidad desconcentrada de la Autoridad de Supervisión del Sistema Financiero a entidad descentralizada bajo tuición del Ministerio de Economía y Finanzas Públicas, específicamente en cumplimiento de la subsistencia, invariabilidad y ejercicio ininterrumpido de sus atribuciones y funciones; establecidos mediante el Decreto Supremo N° 1969 de 9 de abril de 2014; además en cumplimiento al Memorándum de Entendimiento entre los Gobiernos de los Estados del Grupo de Acción Financiera de Sudamérica contra el Lavado de Activos (GAFISUD), aprobado por

Unidad de Investigaciones Financieras
Estado Plurinacional de Bolivia

Ley N° 4072 de fecha 27 de julio de 2009, corresponde aprobar, en base al informe UIF/SIS/33201/2014 de 23 de octubre de 2014, las Políticas de Seguridad de la Información.

POR TANTO:

El Director General Ejecutivo a.i. de la Unidad de Investigaciones Financieras Lic. Victor Hugo Hurtado Vera, Designado mediante Resolución Administrativa N° 044 de fecha 05 de junio de 2015, y en uso de sus facultades y atribuciones.

RESUELVE:

PRIMERO: APROBAR las Políticas de Seguridad de la Información, con sus IX Capítulos, y 5 Anexos, a partir de la emisión de la presente Resolución Administrativa.

SEGUNDO.- La Dirección de Asuntos Administrativos y Finanzas, a través de la Jefatura de Sistemas y Tecnologías de la información queda encargada de la difusión e implantación de la presente Resolución Administrativa y documentos señalados.

Regístrese, comuníquese, cúmplase y archívese.

Lic. Victor Hugo Hurtado Vera
DIRECTOR GENERAL EJECUTIVO a.i.
UNIDAD DE INVESTIGACIONES FINANCIERAS

UNIDAD DE INVESTIGACIONES FINANCIERAS Vo.Bo. J.H.C. JAL

UNIDAD DE INVESTIGACIONES FINANCIERAS V°B° O.U.M. DAFL

UNIDAD DE INVESTIGACIONES FINANCIERAS P.G.T. DAFL

VHHV/JHC/OUM/PGT

CONTENIDO

Unidad de Investigaciones Financieras Vo.Bo. C.I.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

Unidad de Investigaciones Financieras Vo.Bo. C.I.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

3. EQUIPOS DE COMUNICACIÓN
4. ADMINISTRACION DE RECURSOS TECNOLOGICOS
4.1 ALTA DE DISPOCIONES
4.2 MANTENIMIENTO DE DISPOSITIVOS
4.3 MANTENIMIENTO PREVENTIVO
4.4 MANTENIMIENTO CORRECTIVO
4.5 MOVIMIENTO DE DISPOSITIVOS
4.6 INSTALCION FISICA Y CONFIGURACION LOGICA DEL DISPOSITIVO
5. ADMINISTRACION DE FALLAS
5.1 MONITOREO Y CONTROL
5.2 TIPOSDE FALLAS
5.3 FALLADE EQUIPOS CRITICOS
5.4 CAMBIO DE EQUIPOS PRESTADOS
6. ADMINISTRACION DE CLAVES
6.1 RESPONSABILIDAD DE LA CLAVE DE CONFIGURACION
6.2 ALMACENAMIENTO DE LA CLAVE DE CONFIGURACION
6.3 CAMBIO DE LA CLAVE DE CONFIGURACION
7. CONFIGURACION Y CAMBIOS
7.1 AUTORIZACION DE CAMBIOS Y CONFIGURACION
7.2 REGISTRO DE CAMBIOS Y CONFIGURACION
7.3 BITACORA DE COMUNICACIONES
7.4 ADMINISTRACION DE LAS DIRECIONES IP
8. CONTROL DE SEGURIDAD
8.1 SEGURIDAD
8.2 HERRAMIENTAS DE SEGURIDAD
9. ADMINISTRACION DE LA RED
9.1 ADMINISTRACION DE LA CONFIGURACION
9.2 ADMINISTRACION DEL RENDIMIENTO
9.3 DISPONIBILIDAD
10. INFORMACION
10.1 CUSTODIA DE LA INFORMACION
10.2 TRATAMIENTO DE LA INFORMACION SENSIBLE
11. CONTROL DE SEGURIDAD
12. AREAS INVOLUCRADAS
13. INCUMPLIMUIENTO Y SANCIONES

CAPITULO IX – ADMINISTRACION DE PROBLEMATICAS E INCIDENTES

1. OBJETIVO
2. ALCANCE
3. REGISTRO DE PROBLEMAS
4. ARCHIVOS DE INCIDENCIAS
5. DE LOS PROBLEMAS E INCIDENTES
5.1 DEFINICION DE PROBLEMAS E INCIDENTES
5.2 ATENCION DE PROBLEMAS O INCIDENTES EN PRODUCCION (RIESGO/IMPACTO)
6. ESCALAMIENTO
7. REINCIDENCIA O REPETICION

Unidad de Investigaciones Financieras Vo.Bo. C.I.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

8. DOCUMENTACION DE PROBLEMAS E INCIDENTES
9. INFORMACION
9.1 CUSTODIA DE INFORMACION
9.2 TRATAMIENTO DE INFORMACION SENSIBLE
10. CONTROL
10.1 CONTROL DE SEGURIDAD
11. AREAS INVOLUCRADAS
12. INCUMPLIMIENTO Y SANCIONES

ANEXO A ESTACION DE TRABAJO
ANEXO B ACCESOS A INTERNET
ANEXO C FORMULARIO DE SOLICITUD DE INTERNET
ANEXO D FORMULARIO DE SOLICTUD DE RESTAURACION DE PASSWORD
ANEXO F GLOSARIO DE TERMINOS

Unidad de Investigaciones Financieras
Vo.Bo.
C.I.B.
JSTI

Unidad de Investigaciones Financieras
Vo.Bo.
J.L.C.G.
JSTI

CAPITULO I – INTRODUCION

La norma de seguridad TIC contiene los principios y directivas relacionados con la Seguridad de la Información para todos los funcionarios de la Unidad de Investigaciones Financieras (UIF). El propósito de la seguridad de la información es proteger la información contra amenazas relevantes y reducir al mínimo el impacto de los incidentes de seguridad, en lo posible, previniendo su ocurrencia.

1. PRINCIPIOS DE SEGURIDAD DE LA INFORMACION

En las tareas cotidianas que realiza la UIF, poder acceder a la información correcta en el momento adecuado puede marcar la diferencia entre éxito o el fracaso, por lo tanto la UIF reconoce a la información ya a su infraestructura de procedimientos como un bien corporativo clave.

2. ALCANCE

La Norma de seguridad de la Información, procesos y procedimientos asociados deben ser adoptados por toda la UIF.
Por lo tanto, la totalidad de los funcionarios de la UIF, así como las personas que por su relación laboral utilicen recursos tecnológicos de la UIF tienen la obligación de cumplir con las normas, procesos y procedimientos específicos en esta norma.

3. OBJETIVOS

El objetivo de la presente norma de seguridad de la información es:

- Proteger la información del uso no autorizado.
- Asegurar la confidencialidad de la Información.
- Mantener la integridad de la información.
- Asegurar la disponibilidad de la información.
- Cumplir con los requerimientos regulatorios y legales.
- Mantener los planes de continuidad de la infraestructura informática.
- Reportar e investigar todos los incidentes de seguridad de la información.
- Ser la base para las acciones de auditoría.

4. RESPONSABILIDAD

El/la oficial de Seguridad (ver el capítulo II Organización de la Seguridad) tiene la responsabilidad de mantener la documentación técnica, políticas y procedimientos asociados para aportar consejos y dirección de puesta en práctica de la presente norma.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

La responsabilidad de cada funcionario de la UIF ya sea permanente, temporal o a contrato es adherirse a las normas de seguridad de la información, la omisión puede ocasionar daños a la UIF.

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

CAPITULO II - ORGANIZACIÓN DE LA SEGURIDAD

1. OBJETIVO

La presente norma tiene como objetivo administrar la seguridad de la información dentro de la UIF. En este capítulo se definirá un marco de nivel ejecutivo para iniciar y controlar la implementación de la seguridad de la información dentro de la UIF.

2. ALCANCE

La presente norma debe ser aplicada por todo el nivel ejecutivo de la UIF.

3. CONSIDERACIONES GENERALES

Se debe tomar en cuenta que la presente normativa de Seguridad de la Información deberá ser respaldada mediante una Resolución emitida por la Máxima Autoridad Ejecutiva del Unidad de Investigaciones Financieras. Por otro lado la Jefatura de Sistemas y Tecnologías de la Información (JSTI) es la entidad competente para promover y controlar la implementación de las políticas y normativas de la seguridad de la información dentro de la UIF.

AMBITO DE ACCION

La JSTI deberá tener una fuente de asesoramiento especializado en materia de seguridad de la información que estará a cargo del oficial de Seguridad, quien debe ejecutar las siguientes acciones:

- Revisar y proteger a las normas, políticas, Procesos, Procedimientos y las responsabilidades generales en materia de seguridad de la información.
- Monitorear cambios significativos en la exposición de los recursos de información frente a las amenazas mas importantes.
- Revisar y monitorear los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información.

REGULACION

La presente norma tiene por objeto regular, organizar y administrar la seguridad de la información, de acuerdo a las funciones y facultades que este ordenamiento le señale.

PROCEDIMIENTO

La Jefatura de Sistemas y Tecnologías de la Información (JSTI) y la UIF en su conjunto, podrán plantear problemas, sugerencias o peticiones (en materia de seguridad de la información) que se harán en la forma escrita al oficial de Seguridad, esto con el objetivo de mejorar la organización de la seguridad de la información.

Unidad de Investigaciones Financieras Vo.Bo. C.L.C. JSTI

4. JEFATURA DE SISTEMAS Y TECNOLOGIAS DE LA INFORMACION

Las funciones generales de la JSTI en materia de seguridad de información serán:

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

- Revisar y promover mejoras a las Normas, Políticas, Procesos, Procedimientos y las responsabilidades generales en materia de seguridad de la información.
- Promover y controlar la implementación de la seguridad de la información en toda la UIF.
- Aprobar las principales iniciativas para incrementar la seguridad de la información.

5. DESIGNAR AL OFICIAL DE SEGURIDAD

El Director(a) de la Unidad de Investigaciones Financieras en su calidad de máxima autoridad de la UIF designara a un funcionario de la UIF como Oficial de Seguridad.

El/la Oficial de Seguridad debe tener el siguiente perfil:

- Licenciado en Informática, Ingeniero de sistemas o Ramas Afines.
- Experiencia en seguridad y auditoria de Sistemas Informáticos.
- Conocimientos en manejo de redes informáticas y sistemas de comunicación.
- Experiencia de 2 anos en el área de Sistemas Informáticos.
- Conocimiento de la Ley 1178 de Administración y Control Gubernamental
- Cocimiento de las Normas: NB-17799, NB-27002, Cobit , Informe Coso.

5.1 FUNCIONES GENERALES DEL OFICIAL DE SEGURIDAD

El / La Oficial de seguridad deben definir claramente las responsabilidades para la protección de cada uno de los recursos y por la implementación de procesos específicos de seguridad. La política de seguridad de la información debe suministrar una orientación general acerca de la asignación de funciones de seguridad y responsabilidad dentro de la UIF. Esto debe complementarse, cuando corresponda, con una guía mas detallada para sitios, sistemas o servicios específicos. El/La oficial de Seguridad deberá definir claramente las responsabilidades locales para cada uno de los procesos de seguridad y recursos físicos y de información.

El/La Oficial de Seguridad debe coordinar su trabajo con la JSTI y ser asesor en materia de seguridad de la información para la misma. El/La Oficial de Seguridad no debe depender, ni reportar a funcionarios intermedios de la JSTI, debe tener libertad y sobre todo independencia de opinión, por lo tanto El/La Oficial de Seguridad deberá depender exclusiva y únicamente del ejecutivo máximo de la JSTI o una autoridad superior a la citada.

5.2 FUNCIONES ESPECÍFICAS

Las funciones específicas del Oficial de seguridad de la Información serán:

5.2.1 ADMINISTRACION DE LOS CAMBIOS EN PRODUCCION

El / La Oficial de Seguridad debe revisar y evaluar los procesos y procedimientos de Cambios en Producción de sistemas de Información. Entre sus tareas de evaluación, tendrán las siguientes:

- Evaluar la aprobación de los cambios realizados (a nivel de programas y datos) a los sistemas de información que se encuentra en producción.

Vo.Bo. C.I.B. JSTI

Vo.Bo. J.L.C.G. JSTI

- Evaluar la aprobación de las modificaciones en el procedimiento de Cambios en producción.
- Evaluar los reportes de incidentes elaborados por la JSTI y tomar las correspondientes acciones.

5.2.2 ADMINISTRACION DEL PLAN DE CONTINGENCIA

El/La Oficial de Seguridad deberá revisar y avaluar a los procesos y procedimientos referentes al Plan de contingencia. Entre sus funciones tendrá las siguientes:

- Evaluar las mejoras y modificaciones sugeridas en forma interna y/o externa para la mejora de la preparación para la aplicación del plan de contingencias.
- Evaluar las pruebas del plan de contingencia.
- Analizar los reportes de incidentes y resultados de las pruebas elaborados por el Jefe de la JSTI y tomar las correspondientes acciones.

5.2.3 ADMINISTRACION DEL PROCESAMIENTO DE DATOS

Como responsabilidad exclusiva del Oficial de Seguridad, esta la decisión de acción cuando se solicita un cambio con impacto institucional, sea en su autorización o en efectos que conllevan a la Administración de Procesamiento de Datos.

5.2.4 ADMINISTRACION DE PROBLEMAS E INCIDENTES

El /La Oficial de Seguridad deberá revisar y evaluar los procesos y procedimientos de la Administración de Problemas e incidentes. Entre sus funciones tendrá las siguientes:

- Analizar las incidencias reportadas en cuanto al impacto institucional.
- Cuando corresponda solicitar la revisión independiente de los reportes.
- Proponer mejoras y modificaciones para la mejora del servicio de Administración de Problemas e Incidentes.

5.2.5 ADMINISTRACION DE SEGURIDAD INFORMATICA

El/La Oficial de Seguridad deberá realizar la revisión y evaluación a los procesos y procedimientos de la Administración de Seguridad Informática. Entre sus funciones tendrá las siguientes:

- Analizar los incidentes graves en forma puntual.
- Proponer modificaciones y mejoras en el procedimiento.
- Analizar los reportes de rendimiento y disponibilidad.

6. REFORMAS A LA NORMA

La presente norma podrá ser modificada bajo propuesta y presentada formalmente con los correspondientes justificativos al responsable de la JSTI y aprobada por la Dirección de la UIF a través de una resolución.

7. INFORMACION

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

CUSTODIA DE LA INFORMACION

Todos los funcionarios de la JSTI, deben mantener en estricta custodia la información sensible asociada directa e indirectamente a la presente norma.

Toda información es confidencial salvo se exprese lo contrario.

TRATAMIENTO DE INFORMACION SENSIBLE

La información sensible relacionada con la presente normativa, deberá ser conservada durante 12 meses, al cabo de los cuales podrá ser entregado al área de archivo bajo inventario.

8. CLASIFICACION Y CONTROL DE ACTIVOS INFORMATICOS

Para mantener una adecuada protección y control de los activos informáticos de la JSTI, es necesario que sean clasificados.

De acuerdo al Reglamento Especifico del sistema de Administración de bienes y Servicios (RE-SABS), Titulo IV, el manejo de los activos informáticos (equipos) considerados activos fijos o bienes de uso estará a cargo de la Unidad de Activos Fijos.
La JSTI asignara al oficial de Seguridad los bienes informáticos intangibles, como por ejemplo software, cd, dvd, disquetes que contengan información, backup de sistemas, etc.

Por otro lado la información que se almacena dentro de las diferentes bases de datos son exclusivamente propiedad del Unidad de Investigaciones Financieras quedando como custodio de la misma la JSTI.

9. INVENTARIO DE ACTIVOS INFORMATICOS

La toma de inventarios de activos informáticos, de acuerdo al RE-SABS, título IV, artículo 87, tendrá como responsable a:

- Al Jefe de la Unidad de Activos Fijos en caso de bienes de uso (Computadoras Personales, Portátiles, Impresoras, Monitores, bienes intangibles, etc.)
- El Jefe de Sistemas y Tecnologías de la Información en caso de Sistemas informáticos.

10. CLASIFICACION DE LA INFORMACION

La información es como bien intangible valioso, deberá ser clasificada de acuerdo a lo siguiente:

Para fines administrativos o de gestión:
- Por sistema de información
- Por gestión
- Por mes

Para fines de seguridad:
- Información confidencial
- Información interna de la UIF

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

- Información Pública. Se debe asumir que toda información que no esté clasificada, será clasificada como información pública.

ROTULADO DE LA INFORMACION

Para facilitar el inventario de la información almacenada en medios magnéticos como cintas, disquetes, CD, DVD, etc. Se debe rotular la información, el rotulo deberá incluir:

Para fines administrativos o de gestión:

- El sistema de información
- Gestión o año
- Mes

Para fines de seguridad:

- Información confidencial.
- Información Interna a la UIF
- Información Pública. Se deberá asumir que toda información que no lleve ningún rotulo será considerado como información pública.

11. SOLICITUD DE INFORMACION
POR UN FUNCIONARIO O UNIDAD DE LA UIF

Todo funcionario de la UIF que necesite información de otra unidad de la UIF, debe proceder de la siguiente forma:

- Solicitar la Información a través del Jefe de su Unidad.
- La solicitud de información se debe realizar por algún medio que deje rastro o huella , por el ejemplo el correo electrónico, memorando, nota, etc.

Es responsabilidad del dueño de la información (la unidad a la cual se solicita) proporcionar la información clasificada como confidencial.

POR UNA PERSONA EXTERNA A LA UIF

Cuando una persona o entidad externa a la UIF, solicita información a una unidad o dirección de la UIF, se debe proceder de la siguiente manera:

- Deberá estar dirigida según corresponda a Dirección Ejecutiva de la UIF.
- La persona o entidad externa, debe solicitar la información mediante nota y presenta en oficinas de la UIF.

Es responsabilidad del dueño de la información (la unidad o dirección a la cual se solicita la información) proporcionar la información solicitada.

No se podrá proporcionar información a personas o entidades externas a la UIF, que estén clasificadas y/o rotuladas como CONFIDENCIALES y/o INTERNA a la UIF.

Están exentas de esta normativa las certificaciones expresamente reguladas.

12. INCUMPLIMIENTO Y SANCIONES

El incumplimiento a la presente norma será sancionado de acuerdo al reglamento Interno de la UIF referente a Infracciones y Sanciones.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

CAPITULO III – LA SEGURIDAD DE LA INFORMACION

1. OBJETIVO

La presente norma tiene como objetivo garantizar la seguridad, disponibilidad y confidencialidad de la información tomando en cuenta las normas y políticas de la UIF además de la legislación vigente relacionada con la Seguridad de la Información.

2. ALCANCE

La presente norma debe ser aplicada por todo funcionario de la UIF que utilice recursos tecnológicos.

Todo funcionario o persona que trabaja con la UIF debe estar familiarizado con las medidas de seguridad, es evidente que cualquier persona que es funcionario o que trabaja con la UIF puede transgredir las normas y directivas por ignorancia, eso puede tener consecuencias negativas para la UIF.

Por lo expuesto en el párrafo anterior es importante que cada empleado y persona que trabaja con la UIF este en conocimiento de las normas de seguridad de la información, ya que cada persona es responsable que la información sea accesible solamente a personas autorizadas.

3. PROTECCION DE LOS DATOS

Esta norma de protección de los datos se aplica a todo el personal incluyendo la colección, uso, acceso (para Funcionarios y Sujetos Obligados) , destrucción y tenencias de datos. Asegurándose de regirse a los siguientes puntos:

- No divulgar la información referente a casos u otros relacionados.
-
- Asegurarse de que todo usuario que ingresa a cualquier sistema ya sea este funcionario de la UIF o Sujeto Obligado este plenamente identificado y se tenga los datos del mismo.
- Asegúrese de que la información personal este protegida adecuadamente.
- Con el fin de proteger la información de la UIF y tomando en cuenta las características del trabajo que realiza la Unida de Investigaciones Financieras, está totalmente restringido el acceso a las instalaciones, de medios de almacenamiento masivo como ser Discos Duros, PenDrives (Flash Memory), CD/DVD, y otros con características de almacenamiento salvo se tenga las autorizaciones correspondientes para su ingreso y salida.

4. SEGURIDAD DE LAS COMPUTADORAS / MAL USO DE LAS COMPUTADORAS

No está permitido:

- Acceder o intentar tener uso no autorizado a cualquier aplicación informática o estructura de almacenamiento de datos.
- Facilitar el acceso no autorizado a cualquier sistema, aplicación, etc.

- Realizar cualquier acción que cause una modificación desautorizada al contenido de cualquier computador o sistema.
- Realizar cualquier acción que deteriore o interrumpa la operación de cualquier computador.
- Realizar cualquier acción que prevenga u obstaculice el acceso a cualquier programa o datos en cualquier computador.
- Realizar cualquier acción que deteriore la operación de cualquier programa o de la confiabilidad de cualquier dato.
- Nunca se debe acceder a cualquier sistema informático donde el administrador del sistema asignado por la JSTI no le ha asignado un usuario y contraseña autorizada.

5. DERECHOS DE AUTOR, LICENCIAS Y PATENTES

Para propósitos de derechos de autor, los programas de computadora se definen como trabajos literarios y son tema de muchas restricciones.

Para asegurarse de estar dentro la legislación antedicha, queda prohibido copiar o instalar software en equipos de la UIF si no tienen la licencia de uso del software o la autorización de la JSTI.

Si se requiere software adicional para propósitos de la UIF, debe recurrir a plataforma de atención al usuario de la JSTI, quienes se aseguraran de tener el licenciamiento requerido previa instalación del software.

6 INCUMPLIMIENTO Y SANCIONES

El incumplimiento a la presente norma será sancionado de acuerdo al reglamento Interno de la UIF.

Unidad de Investigaciones Financieras Vo.Bo. C.V.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

CAPITULO IV – SEGURIDAD FISICA Y LOGICA

1. OBJETIVO

El objetivo principal de la presente Norma es reglamentar el uso de recursos tecnológicos de la UIF relacionados con la información.

2. ALCANCE

Esta norma debe ser cumplida por todos los funcionarios y consultores que utilizan recursos tecnológicos de la UIF.

3. GENERACION DE CLAVES Y ACCESO A LAS ZONAS DE INFORMACIÓN Y TECNOLOGIA

GENERACION Y CUSTODIA DE CLAVES

El responsable designado, será El/La Oficial de Seguridad, quien debe generar y mantener bajo su custodia, en el Telkey todas las claves correspondientes a dispositivos que poseen la característica de ser administrables por clave y que se encuentren en zonas de información y tecnología.

Se debe definir un periodo equilibrado entre la seguridad y la operatividad para el cambio de claves:

- Las claves de servidores deberán ser modificadas al menos cada 90 días o a la identificación de riesgos.
- Las nuevas claves generadas deberán ser registradas el mismo día del cambio.

CUSTODIO DE LLAVES FISICAS

El responsable designado (oficial de seguridad) debe recolectar y mantener bajo su custodia, en el Telkey, copias y orinales de todas las llaves correspondientes a zonas de información y tecnología, que tengan puertas o muebles, como racks, con este tipo de seguro.

Considerando que las llaves pueden ser copiadas, estas deberán ser cambiadas cuando se considere el riesgo de acceso físico y no se cuente con una medida de control adicional, por ejemplo control de acceso ejercicio por personal de seguridad, chapa adicional con clave o sistema biométrico.

ACCESO A ZONAS DE SISTEMAS (DATA CENTER)

El jefe de la JSTI y el/la Oficial se Seguridad son los únicos funcionarios con acceso que pertenecen a las zonas de sistemas y recursos tecnológicos en cualquier horario.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

El resto de los funcionarios de la JSTI que por sus funciones debe tener un acceso permanente a estas zonas, deberán registrarse y estar autorizado formalmente por el jefe de la JSTI, en el Libro de Registro de Ingreso Data center, estas autorizaciones deben ser revisadas periódicamente.

Cualquier otro acceso adicional a los mencionados beberá estar autorizado y registrado en el indicado Libro y acompañados por el encargado del Data Center.

BAJA DE ACCESOS A ZONAS RESTRINGIDAS

En caso de bajas de personal autorizando para el acceso a las Zonas Restringidas de información y tecnología, la jefatura correspondiente solicitara al respectivo cambio de claves al jefe de la JSTI. La ejecución de esta solicitud deberá realizarse hasta 24 horas después del requerimiento.

CUSTODIO DE ACTIVOS EN ZONAS RESTRINGIDAS

El acceso a cualquiera de las zonas restringidas de información y tecnología por personal no autorizado, ya sea interno a la UIF o externo, deberá realizar bajo la compañía del personal autorizado. En caso de pérdida de algún material, serán responsables el personal a cargo del resguardo de este activo y el acompañante de la visita.

REGISTRO DE ACCESOS

Todas las zonas restringidas de la JSTI deben contar con formas de registro que permita validar la identidad de las personas que acceden o accedieron, el motivo, el funcionario autorizado o acompañante, la fecha, la hora y otros datos que hagan de este registro más exacto.

4. MANTENIMIENTO

MANTENIMIENTO Y LIMPIEZA DEL CENTRO DE PROCESAMIENTO DE DATOS (CPD).

Las tareas de mantenimiento y limpieza del CPD, deben contar con la autorización del Jefe de la JSTI, y es responsable de supervisar esta actividad el encargado del centro de datos o en su defecto el Jefe de la JSTI podrá designar un responsable que valide la correcta y segura ejecución de la tarea.

EXTINGUIDORES Y ALARMAS CONTRA INCENDIO

Todas las zonas restringidas deberán contar con extinguidores y alarmas contra incendio en lugares visibles y accesibles. El Jefe de la JSTI deberá coordinar el mantenimiento de este equipo con la Unidad correspondiente.

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

5. TELKEY

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

El telkey es considerado como zona restringida de Información y Tecnología, consecuentemente debe ser controlado bajo la responsabilidad del oficial de Seguridad en caso de que la UIF contemple la implementación de un telkey se deberá tomar en cuenta lo siguiente.

Se debe registrar todo ingreso, cambio o retiro de sobres lacrados en el Telkey.

Todo sobre que ingrese deberá conectar la fecha de caducidad y ser retirado a su cumplimiento.

Cada titular de clave o llave física es responsable del contenido del sobre entregado.

6. CUENTAS DE USARIOS TECNICOS

ADMINISTRACION DE USUARIOS TECNICOS

La JSTI administrara las cuentas de los usuarios técnicos necesarios para la administración de Servidores, aplicaciones, dispositivos de telecomunicación y otros dispositivos.

Todo funcionario autorizado que trabaje con recursos tecnológicos recibirá una cuenta de usuario técnico como parte de sus responsabilidades.

Para la baja o traspaso de una cuenta de usuario técnico se deberá contar con la autorización del jefe de la JSTI y si corresponde, por ejemplo ante el retiro del funcionario titular de la cuenta, la supervisión del Oficial de Seguridad.

Cuando se considere necesario se podrá dividir la contraseña de una cuenta en 2 partes y asignar cada parte a un funcionario distinto, privilegiando la segregación de funciones y oposición de intereses, esta medida podrá ser aplicada principalmente a cuentas muy sensibles o de alto riesgo.

7. SEGURIDAD LOGICA

ACCESOS REMOTOS

Ningún funcionario de la JSTI podrá tener habilitado un acceso remoto con facilidades de administración a ningún recurso o aplicación informática sin la debida autorización del Jefe de la JSTI y/o el/la Oficial de Seguridad de la Información.

UTILITARIOS Y SOFTWARE DE ADMINISTRACION

Ningún funcionario de la JSTI podrá tener instalado o hacer uso de utilitarios o software de administración por ejemplo: sniffers o rastreadores lógicos, que no estén debidamente licenciados y autorizados por la jefatura de la JSTI y/o el/la Oficial de Seguridad de la Información.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

8. INFORMACION

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

CUSTODIA DE LA INFORMACION

El personal de la JSTI debe mantener en estricta custodia la información asociada directa e indirectamente a la presente norma. Toda la información contenida en la presente normativa es considerada confidencial salvo el titular exprese lo contrario.

DEL TRATAMIENTO DE INFORMACION SENCIBLE

La información impresa relacionada con la presente normativa, deberá ser conservada durante 12 meses, al cabo de los cuales podrá ser entregada a la unidad de archivo correspondiente bajo inventario. La información en medios digitales quedara bajo resguardo de la JSTI sujetas a disposiciones legales en cuanto a término y plazos de custodia.

9. CONTROL

CONTROL DE SEGURIDAD

Todos los funcionarios deberán velar por el estricto cumplimiento de la presente normativa, siendo su responsabilidad denunciar cualquier sospecha o cumplimiento de violación a lo establecido ante el/la Oficial de seguridad y procurar su aclaración.

REVISION

El/la Oficial de Seguridad es responsable de efectuar revisiones y evaluaciones de la seguridad tanto físicas como lógicas de la JSTI, así como del correcto uso y explotación de los recursos tecnológicos.

10. AREAS INVOLUCRADAS

Las áreas involucradas en la presente norma, son:

Jefatura de la JSTI

- En la aprobación de los derechos de acceso físico y lógico del personal de Información y Tecnología.
- En la revisión y validación de los accesos registrados a las zonas de Información y tecnología.

Oficial de Seguridad

- Generación de los reportes
- Autorización de accesos físicos y lógicos en coordinación con la jefatura de la JSTI.
- En la revisión de los derechos de acceso físico y lógico del personal de Información y Tecnología.
- En la revisión del Telkey.

Personal de la JSTI

- En la actualización de contraseñas en el Telkey.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

- En el cumplimiento estricto de la presente normativa.

11. INCUMPLIMIENTO Y SANCIONES

El incumplimiento a la presente norma será sancionado de acuerdo al reglamento Interno de la UIF referente a Infracciones y Sanciones.

Unidad de Investigaciones Financieras Vo.Bo. C.L.S. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

CAPITULO V – LA ESTACION DE TRABAJO

1. OBJETIVO

El objetivo de la presente norma es regular el uso de las computadoras personales y portátiles dentro de la UIF.

La UIF proporciona a su personal una estación de trabajo (computadora de escritorio o portátil), el mismo que tiene instalado el software estándar requerido, por lo que cada funcionario de la UIF es responsable de su estación de trabajo y por lo tanto debe cumplir con lo indicado en el presente capitulo.

2. ALCANCE

Esta norma debe ser cumplida por todo funcionario, consultor o personas que trabajan en la UIF, que utiliza un equipo de computación proporcionado por la UIF.

3. LA COMPUTADORA ESTA PARA TRABAJAR

La computadora y todos los recursos a disposición deben ser utilizados exclusivamente para fines profesionales. Se debe evitar especialmente el uso indiscriminado del correo electrónico, este medio de comunicación puede ser auditado en cualquier momento, no apoye objetos sobre los computadores y evite comer y/o beber mientras la utiliza.

4. INSTALACION DE SOFTWARE

No esta permitido instalar software personal o de negocio en su PC o computadora portátil por las siguientes razones:

- El programa puede contener un virus.
- El software puede afectar el rendimiento de su PC.
- El licenciamiento del software no esta contemplado en el software corporativo de la UIF.
- Puede haber disponible un producto alternativo del estándar de la UIF.

Si requiere instalar otro software para los propósitos de la UIF, debe contactar a plataforma de atención al usuario de la JSTI.

5. PROTECTORES / FONDOS DE PANTALLA

No esta permitido instalar protectores o fondos de pantalla en la PC. Solamente los fondos o protectores de pantalla autorizados o proporcionados por la JSTI.

Cualquier otro fondo o protector de pantalla será desinstalado por funcionarios de la JSTI.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

6. PROTECION DE SU ESTACION DE TRABAJO

Se debe bloquear siempre la estación de trabajo cuando se ausente de su escritorio.

Además se debe de activar el bloqueo automático cuando su PC esta inactiva por aproximadamente por 5 minutos.

Debe grabar y cerrar los documentos y aplicaciones con los que esta trabajando antes de dejar su escritorio.

7. APAGUE SU COMPUTADOR AL RETIRARSE DE LA OFICINA.

al finalizar la jornada de trabajo siempre se debe apagar el computador personal por completo

8. VACIAR PAPELERA DE RECICLAJE

Se debe vaciar la papelera de reciclaje del sistema operativo cuando baya a borrar archivos con información confidencial. Es extremadamente sencillo recuperar la información de esta papelera si no se realiza esta operación. Esta se debe convertir en un habito al menos una vez por semana.

9. ORDEN Y ORGANIZACIÓN DE LA INFORMACION

Debe mantener en orden su información. Para ello, el SO provee de herramientas para organizar y depurar la información Ante cualquier duda contáctese con plataforma de atención al Usuario de la JSTI.

Periódicamente y en función a la importancia de la información que guarda en su PC, debe solicitar a la plataforma de atención al usuario de la JSTI la realización de un Backup de sus archivos más importantes.

10. ACCESO A LA ESTACIÓN DE TRABAJO

Cada funcionario de la UIF cuenta con un nombre de Usuario y código personal (Usuario y Password) para acceder a una estación de trabajo, es importante que este código lo utilice solo la persona a la cual le fue asignada, y no lo preste a nadie. **El uso de su Nombre de Usuario y código (Password) es responsabilidad del funcionario al cual se le asigno el código,** si se tiene la impresión que el código está siendo utilizado por otra persona se debe reportar de inmediato a la JSTI o al Oficial de Seguridad

11. USO DE COMPUTADORAS PORTÁTILES

Todo funcionario o persona que utilice un computador de la UIF debe cumplir lo siguiente:

Unidad de Investigaciones Financieras Vo.Bo. C.U.S. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

CONTRASEÑAS

Se debe configurar una contraseña de inicio antes de que se active el sistema, de esta manera se evitara arriesgar los datos. Si no sabe como, contáctese con la JSTI.

El protector de pantalla debe estar configurado con contraseña.

BACKUPS

Cuando almacene documentos estos debe de realizarlos en la Unidad D u otra unidad de disco duro diferente de la Unidad C (sistema operativo), Si no sabe como, contáctese con la JSTI.

ACCESO A INTERNET POR MODEM

Está prohibido conectarse a Internet a través de un módem, ya que el mismo no está protegido por los controles de seguridad comprendidos por la UIF.

SEGURIDAD FÍSICA

Debe asegurarse lo siguiente:

- Guardar bajo llave su portátil al retirarse de su oficina
- Cuando se encuentre de viaje lleve, su portátil con el equipaje de mano
- No lleve consigo información confidencial en otros bolsos

El funcionario es responsable de la computadora portátil mientras está en su posesión. La falta de proteger adecuadamente este equipo y/o los sistemas y datos almacenados en el equipo, podría dar lugar a una acción disciplinaria

12. INCUMPLIMIENTO Y SANCIONES

El cumplimiento a la siguiente norma será sancionado de acuerdo al Reglamento Interno de la UIF.

CAPITULO VI - USUARIOS Y CLAVES DE ACCESO

1. OBJETIVO

La presente norma tiene como objetivo definir los controles necesarios que los usuarios deben ejercer, para mantener un adecuado nivel de seguridad, durante la utilización de los recursos tecnológicos y los servicios disponibles para el cumplimiento de sus funciones.

Los servicios disponibles para los objetivos de la UIF deben ser utilizados para fines institucionales. Estos podrán ser utilizados para fines personales de una manera razonable y controlada siempre y cuando no perjudiquen los servicios y procesos de la UIF.
El/La Oficial de Seguridad definirá anualmente los parámetros para considerar el uso de estos servicios como razonables y no perjudiciales para la UIF.

2. ALCANCE

Esta norma debe ser cumplida por todos los funcionarios, personal a contrato y toda persona que trabaje con un computador personal proporcionado por la UIF.

3. COMPUTADORAS PERSONALES

3.1 CUSTODIOS Y USO DE COMPUTADORES PERSONALES Y PERIFÉRICOS

Los computadores y periféricos son asignados por la Unidad de Activos Fijos para uso a un área o a un usuario específico. Cada dispositivo debe tener asignado un responsable para el correcto uso del mismo. Los equipos de la UIF solo deben usarse para actividades laborales o de interés institucional.

3.2 ACCESO LÓGICO

Todos los computadores personales deben tener habilitadas las contraseñas de acceso al sistema operativo y la contraseña de acceso a la red de la UIF. Cada usuario es responsable de las claves asignadas a su persona.

La contraseña como administrador del PC (setup) estará administrada por el encargado de plataforma de atención al cliente (soporte técnico) de la JSTI. Cuando sea técnicamente posible.

Unidad de Investigaciones Financieras Vo.Bo. C.L.G. JSTI

3.3 INFORMACIÓN ALMACENADA

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

Toda la información recibida, procesada y almacenada en cualquier medio de retención, disco duro, memoria electrónica, memoria óptica, y otros, es de absoluta propiedad de la UIF. Los custodios de dispositivos son responsables de su cuidado, manteniendo adecuados niveles de integridad, disponibilidad y confidencialidad.

Entre las responsabilidades para los usuarios tenemos:

- Todos los datos de los usuarios deben estar almacenados en las carpetas establecidas por la JSTI.
- Si el software instalado graba por defecto en otro lugar, el usuario debe solicitar a través de la plataforma de atención al usuario, la configuración para que las grabaciones se hagan en el lugar indicado.
- Los respaldos son realizados en forma automática en aquellos equipos cuyas características lo permiten y siempre que haya sido coordinados con la JSTI. La jefatura de la JSTI a solicitud expresa del usuario realizará la copia manual de aquellos equipos que no cuentan con la facilidad de hacerlo automáticamente. Los respaldos generados estarán centralizados en la JSTI y administrados por cuotas.
- Cuando un usuario tenga la necesidad de realizar respaldos adicionales que no serán custodiados por la JSTI, debería solicitar autorización del Oficial de Seguridad, para que el encargado de Plataforma de atención al usuario haga copias periódicas o únicas y se las entregue.
- Cuando el dispositivo es reemplazado por otro, el custodio debe verificar que la información del dispositivo reemplazado esta correctamente replicado, debiendo especificar su conformidad en el plazo de 24 horas.
- Con el fin de precautelar la información residente en los equipos los usuarios no deben copiar a un medio removible, el software o borrar los datos residentes.
- Tomando en cuenta la información que maneja la UIF, los periféricos y unidades de medios removibles se encontraran deshabilitados, y se habilitaran medios de almacenamiento bajo registro de la JSTI.
- Los periféricos de los equipos asignados a los usuarios con categoría de Director inicialmente se encuentran habilitados, pudiendo estor ser bloqueados a solicitud del mismo o de la Máxima Autoridad Ejecutiva de la UIF.
- Cuando juzgue necesario la Jefatura de la JSTI podrá deshabilitar todos los periféricos y unidades de medios removibles.
- No pueden extraerse datos fuera de la UIF sin la aprobación previa y escrita de la Dirección Ejecutiva de la UIF o a quien se delegue esta responsabilidad.
- Si el intercambio de información es resultado de un contrato de prestación de servicios o requerimientos regulatorios o legales o convenios interinstitucionales no será necesaria la aprobación previa ni escrita, ya que la misma deberá utilizar otros medios de intercambio (VPN, Web Service, otros).

Unidad de Investigaciones Financieras Vo.Bo. C.L.G. JSTI

3.4 SOFTWARE INSTALADO

A menos que se indique lo contrario, los usuarios deben asumir que todo el software instalado en los equipos de la UIF está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y esta terminantemente prohibido, hacer copias o usar este software para fines personales o instalar en cualquier equipo interno o externo sin la autorización de la JSTI o el/la

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

Oficial de Seguridad. La instalación deberá ser solicitada a través de la plataforma de atención al usuario.

3.5 CONFIGURACIÓN

Debe respetarse y no modificarse la configuración de hardware y software establecida por la JSTI:

- Está prohibido que el funcionario cambie alguna parte de la computadora como ser: teclado, mouse, monitor, CPU, impresora y otros, sin la solicitud y aprobación de la Unidad de Activos Fijos.
- Los usuarios no deben cambiar la configuración establecida, desactivar aplicativos de control y prevención como antivirus, software auditoria, programas de inicio (logon scripts) o cualquier herramienta o utilitario instalado por la JSTI.

3.6 PROTECTOR Y FONDO DE PANTALLA

La JSTI establecerá mediante dominio el conjunto de protectores y fondos de pantalla a ser utilizados.

3.7 CUIDADO FÍSICO

El custodio designado velará por la integridad física de los recursos tecnológicos, debiendo cumplir lo siguiente:

- Existan los medios de protección necesarios de acuerdo con el ambiente u oficina que tenga. Estos medios pueden comprender cobertores, conexiones antiestáticas, oficinas con llave u otros.
- Todo movimiento necesario que signifique el cambio de ubicación física debe ser solicitado a la UNIDAD DE ACTIVOS FIJOS, quien coordinará con la JSTI para realizar el ajuste de las conexiones necesarias.
- El custodio puede, solo bajo circunstancias de peligro inminente como incendio, inundación u otros, retirar o resguardar partes de una computadora y/o periféricos.
- La pérdida o robo de cualquier componente de hardware debe ser reportada inmediatamente a la Unidad de Activos Fijos quienes deben informar al Jefe de Seguridad Fisca de la UIF y otras áreas que corresponda.
- Cualquier anormalidad detectada con relación a la configuración o estado físico, debe ser comunicada inmediatamente a la JSTI a través de la plataforma de atención al usuario.

4. SEGURIDAD LÓGICA

4.1 USER ID

El User-ID del sistema deberá ser único por usuario y de ninguna manera un usuario podrá tener dos user-id para acceder a los sistemas. En situaciones donde no exista posibilidad y el usuario deba tener más de un User-ID se deberá proceder según el principio de "segregación de funciones que privilegie la oposición de intereses" y se deberá contar con la autorización formal del Oficial de Seguridad.

Unidad de Investigaciones Financieras Vo.Bo. C.I.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.I.C.G. JSTI

El User-ID debe estar vinculado a una persona y su longitud no debe ser menor a cuatro caracteres. Las cuentas genéricas como mínimo deben cumplir las siguientes condiciones:

- Asignadas al Jefe de Unidad como responsable
- Solamente podrán permitir consulta y recuperación de datos autorizados por el jefe de la unidad
- No deben tener acceso a generadores de consulta ad-hoc (SQL o similares)

4.2 CLAVES DE ACCESO

Las claves de acceso deberán tener un mínimo de seis caracteres. Estas no deberían estar relacionadas al trabajo o a la vida personal, los nombres personales, lugares y otros.

- Está prohibido construir claves de acceso con ciertos caracteres que no cambien o que cambien de manera predecible, por ejemplo meses (X31ENE, X31FEB), proyectos, departamentos y otros.
- No se debe crear claves que son idénticas o sustancialmente similares a las claves empleadas anteriormente.
- Una clave deberá contener caracteres tanto alfabéticos como numéricos.
- La clave no deberá tener más de dos caracteres iguales juntos. Es recomendable que contenga mayúsculas y minúsculas ya que dificulta su descifrado por personas no autorizadas.
- Las claves deberán ser modificadas al menos cada 90 días para prevenir el descifrado de la misma por terceros. Cuando sea factible técnicamente, el sistema deberá generar automáticamente una alarma informando que clave caducará. Antes de su vencimiento, se emitirá un aviso cada vez que el usuario ingrese a los sistemas informáticos de la UIF. El usuario es responsable de cambiar su clave durante este periodo de pre aviso y no podrá crear una clave igual al menos a las últimas cinco que utilizó anteriormente.
- El número de intentos para ingreso de esta clave está limitado a tres intentos. En caso de contarse con tres intentos fallidos y ser factible tecnológicamente, se suspenderá la cuenta de dicho usuario y será rehabilitada por la JSTI con la respectiva solicitud de restauración de password (ver Formulario de solicitud en anexos).

Cuando se sospeche que personas no autorizadas han descubierto su clave es necesario cambiarla inmediatamente o solicitar ayuda al personal de la JSTI. Las claves que se utilizan son personales y secretas. Considerando las circunstancias, las claves no deben ser compartidas y reveladas a ninguna persona. Hacerlo expone al usuario autorizado a asumir las responsabilidades por todas las acciones realizadas con esa clave. Los usuarios son responsables por todas las actividades realizadas con sus User-ID y claves de acceso.

En los casos donde el administrador del sistema asigna una clave inicial (Por Ejemplo: cuentas nuevas de correo electrónico, rehabilitación de claves), el usuario esta en la obligación de cambiar en la primera sesión su clave.

4.3 NORMAS PARA VALIDACION DE CLAVES DE ACCESO

Para la validación de claves de acceso, se debe cumplir lo siguiente:

- Las contraseñas o claves de acceso se deben cambiar regularmente cada noventa días o menos, por lo tanto en función de que la tecnología permita, los Servidores deben configurarse para caducar la contraseña en ese periodo.
- la restauración de Passport debe de solicitarse mediante formulario de Restauración de Password
- La longitud mínima de una contraseña es de seis caracteres para lo cual deberá utilizar mayúsculas, minúsculas, números y un carácter especial ($,%,&).
- No pueden habilitarse contraseñas utilizadas anteriormente para el mismo código de usuario (hasta las últimas 10).
- No pueden repetirse caracteres en la misma posición que la contraseña anterior (por ejemplo: no se puede habilitar la contraseña JUAN2 si la contraseña anterior fue JUAN2).

4.4 USO DE LA CLAVE DE ACCESO

- Se debe utilizar contraseñas que no puedan ser adivinada fácilmente por otras personas. La contraseña no debe contener ninguna información personal (es decir su nombre, fecha de nacimiento, nombre de familiares, etc.).
- Debe cambiar su contraseña con regularidad.
- No divulgue su contraseña a ninguna persona. Si sospecha que alguien sabe su contraseña, informe a la JSTI a través de plataforma de atención a usuario o al oficial de seguridad inmediatamente.
- Tenga cuidado al ingresar su contraseña, asegúrese que no esta siendo observado.
- Si sospecha de algún uso no autorizado de su contraseña reporte el mismo al Oficial de Seguridad de la Información

4.5 ATENCION DEL PC

Los usuarios no deben dejar sus computadoras (PC) sin antes realizar un proceso de cierre de sesión o habilitar el bloqueo de equipo.

El bloqueo de equipo deberá estar configurado para activarse al menos en diez minutos. Solamente están permitido el protector o fondo de pantalla proporcionado por la JSTI

Cualquier otro fondo/protector de pantalla no autorizado será desinstalado por la JSTI.

4.6 DIRECTORIOS E INFORMACION COMPARTIDA

Los usuarios no deben compartir directorios de sus equipos. Está prohibido compartir todo el disco de un equipo, porque puede comprometer la información del sistema operativo, aplicaciones y otros, ocasionando daños al equipo.

Si es necesario compartir información residente en un equipo, deberá utilizarse el correo electrónico o directorios públicos (compartidos con claves de acceso obligatoriamente).

La UIF en la actualidad cuenta con un servidor para compartir archivos, todos los usuarios que tienen acceso a la red pueden colocar sus archivos para compartirlos en este servidor, esta

prohibido colocar archivos de música (MP4,MP3 y otros parecidos), videos y archivos que no están relacionados al trabajo de la UIF.

5. NORMAS DE SEGURIDAD FISICA

Todos los ambientes de la JSTI deberán contar con acceso restringido al personal no autorizado. Se entiende por personal autorizado con acceso a estos ambientes a:

- Al personal de la JSTI asignado a tareas específicas que se deban realizar en estas instalaciones.
- Al personal expresamente designado
- Al Oficial de Seguridad

Personas que no pertenezcan a la JSTI deberán solicitar permiso de acceso a la jefatura de la JSTI para acceder a los Ambientes de Computo (Data Center). El ingreso de personal no autorizado debe ser registrado.

6. DEL ACCESO A INTERNET

6.1 NORMA – ACCESO A INTERNET

Todos los accesos a Internet deberán ser solicitados formalmente a la Jefatura de la JSTI contando con la autorización de su respectiva Jefatura y otros consignados en el formulario de solicitud (Ver Anexos).

6.2 CONTENIDOS AUTORIZADOS

Los funcionarios deberán visitar únicamente páginas que estén relacionadas con sus funciones o con los intereses institucionales. Esta terminantemente prohibido visitar páginas cuyos contenidos atenten contra la moral, buenas costumbres, imagen del hombre, la mujer o los niños.

La UIF a través de la JSTI se reserva el derecho de utilizar medios y herramientas informáticas para controlar, bloquear y/o monitorear los contenidos accedidos mediante su red interna independientemente del horario, el cargo o la jerarquía del funcionario o usuario.

6.3 DESCARGA DESDE INTERNET

Los funcionarios no deberán descargar material, información, software o datos de páginas de dudoso o desconocido origen por el peligro de virus, violación de la propiedad intelectual o daño a la moral, buenas costumbres o imagen de la UIF.

De igual manera no se deberán descargar grandes volúmenes de datos en horarios laborales por la saturación de tráfico que puedan ocasionar.

Si se considera necesario la JSTI podrá definir de manera semestral los parámetros de uso y administración de este servicio.

6.4 ENVIO DE INFORMACION POR INTERNET

Los usuarios no deben enviar información confidencial de la UIF vía Internet, por ejemplo contraseñas, claves de accesos, números de cuenta o PIN's. En caso de existir la necesidad, por ejemplo de una compra por Internet, deberán solicitar por la plataforma de atención al usuario la ayuda y colaboración de personal de la JSTI y cuando corresponda con la autorización del Oficial de Seguridad.

6.5 MENSAJERIA INSTANTANEA POR INTERNET

El acceso a servicios de mensajería instantánea por Internet es de uso exclusivo de las Direcciones y Jefaturas de la UIF y para el caso de un funcionario que lo requiera este deberá contar con la respectiva autorización de su respectiva Dirección y Jefatura debiendo justificar su necesidad para fines de la UIF, y el mismo solo podrá ser por un tiempo limitado. Una vez autorizado, la Jefatura de la JSTI podrá habilitar el mismo de acuerdo a las políticas vigentes en la UIF.

Este servicio no debe comprometer la confidencialidad de la información y debe ser utilizado únicamente para facilitar la comunicación continua y no así para otros fines. El envío o recepción de archivos debe realizarse vía correo electrónico para garantizar los principios de confidencialidad y no repudio.

6.6 ACCESO A INTRANET

Todos los funcionarios de la UIF que requieran de acceso a la intranet, deben solicitarlo de forma escrita a la JSTI o a través del correspondiente formulario (ver anexos).

El encargado de los equipos que proveen internet deberá llevar registro y control de todos los funcionarios de la UIF que tienen acceso a Internet y qué tipo de acceso.
Los mismos que pueden ser del siguiente tipo:

TIPO 1.- Accesos a Full Internet, sin restricción de páginas y cuenta de correo externo habilitado. (el mismo que será habilitado a las máximas autoridades de la UIF)

TIPO 2.- Acceso a Internet, restricción y control de paginas categorizadas y no categorizadas.

TIPO 3.- Acceso a Internet, restricción y control de paginas categorizadas

TIPO 4.- Acceso a Internet, solo a sitios web del Estado Plurinacional de Bolivia.

los/las usuarios de la UIF deben considerar que el uso del internet y el acceso a sitios no autorizados es enteramente responsabilidad del funcionario solicitante.

Unidad de Investigaciones Financieras Vo.Bo. C.L.C. JSTI

6.7 CONTENIDO Y USO DEL MATERIAL

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

La intranet implementada tendrá el objetivo de facilitar la comunicación interna con información relacionada con las tareas cotidianas de la UIF. Todos los funcionarios deben visitar regularmente la Intranet con la finalidad de conocer e informarse del material que está disponible por este medio.

La JSTI debe implementar mecanismos para implementar por defecto la aparición de la intranet de la UIF en todos los navegadores de Internet (Internet Explorer) de los usuarios de la UIF.

La Administración técnica de la Intranet es responsabilidad del Administrador de Servidores de la JSTI y el Analista de Soporte de Datos , sus principales responsabilidades serán:

- Mantener y administrar el servidor donde funciona la intranet de la UIF.
- Obtener copias de respaldos de toda la intranet de la UIF y probar que las copias de respaldo funcionen.

Todas las unidades deben tener acceso a la Intranet de la UIF, con el objetivo de poder incluir, modificar o eliminar contenido, la autorización para realizar tareas antes mencionadas deben ser solicitadas al administrador de servidor de la JSTI, a través de un medio que deje huella (correo electrónico), teniendo cada solicitante la responsabilidad sobre el contenido del mismo.

El/la Oficial de Seguridad debe validar regularmente los contenidos disponibles en la Intranet.

6.8 CONFIDENCIALIDAD DE LA INFORMACION

La información de la Intranet es confidencial y su uso y conocimiento esta permitido únicamente a los funcionarios de la UIF o personas autorizadas. La información obtenida en la Intranet puede salir de la institución únicamente para fines de la UIF con la autorización de la unidad que corresponda.

7 SERVICIOS ADICIONALES

7.1 PRESTAMO DE DISPOSITIVOS MOVILES

Los dispositivos móviles tales como: equipos multimedia, computadores portátiles, proyectores u otros; deben ser solicitados al titular del dispositivo móvil quien será responsable de entregarlos y recibirlos de vuelta validando su correcto funcionamiento.

El funcionario solicitante es responsable de los mismos mientras estos estén bajo su custodia. La solicitud de préstamo deberá hacerse mínimo con 3 horas hábiles antes de su uso requerido.

Cuando el funcionario solicitante necesite sacar el dispositivo móvil fuera de los ambientes de la institución, deberá seguir las normativas internas sobre movimiento o salida de activos.

8. DEL ANTIVIRUS

El custodio o usuario es responsable por la grabación de archivos o programas cuando estos no son instalados por la JSTI.

El usuario debe solicitar al momento recibir el computador la información sobre el Antivirus instalado, de igual manera esta precaución debe repetirse cuando se realiza el mantenimiento preventivo o correctivo.

El usuario final no puede realizar ningún mantenimiento, debe solicitarlo a través de plataforma de atención al usuario de la JSTI cuando este se considere necesario.

Los usuarios que cuentan con Internet o correo electrónico deben validar y constatar La fuente o remitente de un mensaje o página Web antes de iniciar una descarga de archivos o abrir un correo electrónico con archivos adjuntos.

El custodio o usuario no debe instalar ningún tipo de programa, imagen, música o archivos de video en su computador sin la autorización de la JSTI y/o el/la Oficial de Seguridad.

Ante la detección de virus mediante la alarma del programa antivirus, el custodio o usuario debe seguir las instrucciones que el programa sugiere, si no esta seguro del efecto a producirse debe colocar una solicitud de atención mediante la plataforma de atención al usuario. Cuando el usuario recibe noticias sobre la aparición de virus por cualquier medio, no debe tomar acción alguna, más que validar que posee un programa antivirus instalado en su computador. Adicionalmente debe comunicar a la Jefatura de la JSTI sobre la noticia y puede solicitar atención mediante la plataforma de atención al usuario pero de ningún modo tomar acción alguna.

9. DEL LICENCIAMIENTO Y USO DE SOFTWARE LEGAL

9.1 UTILIZACION DE SOFTWARE SIN LICENCIA

La UIF, acorde a sus principios y valores de respeto por la propiedad intelectual y por los derechos de autor, prohíbe la utilización, ejecución o almacenamiento de software sin licencias en todas las computadoras pertenecientes a la institución.

9.2 ACTUALIZACION DE VERSIONES

Si no se cuenta con una licencia de actualización de software, la ejecución de la nueva versión es ilegal. Por lo tanto, queda prohibida la actualización de versiones de software que no estén autorizados por la JSTI.

9.3 RESPONSABILIDAD POR SOFTWARE ILEGAL (SIN LICENCIA)

El usuario no debe instalar software en su equipo sin la aprobación previa de la JSTI. En caso de que el equipo sea utilizado por dos o más personas, esta responsabilidad estará en la persona a la cual se le asigno el equipo. De esta manera, cualquier software ilegal (sin licencia) que pueda ser identificado en computadoras de la UIF, será de completa responsabilidad del usuario.

Unidad de Investigaciones Financieras Vo.Bo. C.L.G. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

Cualquier daño legal o de diferente naturaleza que cause a la UIF, deberá ser respondido en su integridad por el usuario, según el Reglamento Interno.

La JSTI realizará un control de seguimiento al software instalado en cada máquina según normas interna de la JSTI.

9.4 UTILIZACION DE SOFTWARE QUE NO REQUIERE LICENCIA

En caso de existir software que no requiera licencia (freeware, shareware, open source) podrá ser utilizado por los funcionarios de la UIF previa autorización de la JSTI.

9.5 AUTORIZACION PARA COPIAS DE SEGURIDAD

La JSTI es el único autorizado para generar copias de seguridad del software de la UIF. Estas copias podrán ser utilizadas para la instalación de software en las computadoras de nuestra institución respetando los planes de licenciamiento establecidos.

9.6 EVALUACION DE COMPUTADORAS DE LA UIF

La JSTI cuenta con autorización para evaluar las computadoras pertenecientes a la UIF respecto al software que tiene instalado, verificando que únicamente tenga almacenado el software autorizado. Asimismo esta facultado para elaborar informes al respecto a la Dirección o Unidad que corresponda. La JSTI comunicará al Oficial de Seguridad sobre la trasgresión de la norma y procederá a actualizar el software según el perfil respectivo.

9.7 MEDIOS DE ALMACENAMIENTO

Los usuarios no podrán tener en sus puestos de trabajo ningún medio de almacenamiento con programas y/o instaladores de aplicaciones (CD's, disquetes, cintas, etc.) sean estos originales o copias.

Todos estos medios de almacenamiento deberán ser inventariados y almacenados en la JSTI. Los únicos medios de almacenamiento que se autoriza al usuario tener en su poder, son aquellos que contienen datos e información relacionada a la operativa de la UIF y cuenten con la autorización formal.

10 ALTAS, BAJAS, MODIFICACIONES Y BLOQUEOS DE USUARIOS

10.1 SOLICITUD DE MOVIMIENTO DE CUENTAS

El área responsable de solicitar altas, bajas y bloqueos de los usuarios es la Unidad de Recursos Humanos. Esta dirección solicitará el movimiento de cuentas (Se entiende por el movimiento de cuentas a la operación de alta, modificación y baja o bloqueo de cuentas de usuarios), a la JSTI. La Dirección de la UIF también puede solicitar movimientos de cuentas.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.V.C.G. JSTI

Las modificaciones de acceso podrán ser solicitadas por la Dirección o Unidad que corresponda al usuario. Para todas las soluciones, se utilizará un formulario impreso diseñado exclusivamente para este fin donde se completará la sección que corresponda para luego ser entregado a la JSTI.

A todo el personal que sea contratado por la UIF que no sea de planta (consultores) se deberá asignar una cuenta de usuario que expire en la fecha que termine su contrato.

10.2 EJECUCION DE LAS SOLICITUDES

Toda solicitud de usuario ante la JSTI deberá realizarse mediante **Formulario de habilitación de Usuario** adjunto en los Anexos de la presente norma.

La jefatura de la JSTI asignará la solicitud según corresponda:

- Para acceso a la red de la UIF
- Para correo electrónico
- Para acceso a Internet
- Para Mensajería interna/externa
- Para acceso a la Intranet
- Para acceso a un sistema de información

Se ejecutará las solicitudes completando el resto del formulario de solicitud y actualizando los datos del usuario en el sistema en cuestión. El formulario impreso debe ser archivado por la Jefatura de la JSTI, que posteriormente deberá comunicar al usuario su clave de "Acceso Trivial" de los cambios o asignaciones realizadas.

10.3 SOLICITUD DE RESPALDO DE INFORMACION EN CASO DE DESVINCULACION

Todo funcionario que este dejando la institución de manera permanente, esta prohibido de borrar información que se genero en su equipo, en caso de borrar o extraer alguna información, la UIF procederá a iniciarle las acciones legales o administrativas que corresponda. Las unidades involucradas en la presente disposición deberán cumplir lo siguiente:

- Datos en los equipos del usuario: ante solicitud del área responsable de trabajo del usuario, la JSTI respaldará y entregara al área solicitante la información que usuario pueda haber generado y/o utilizado en el disco duro de su equipo.

La JSTI no se responsabilizará de la información del usuario que fue dado de baja, en caso de no existir un requerimiento formal para respaldar esta información hasta 48 después de solicitada la baja permanente del usuario.

- Disponibilidad de Equipos: los equipos que el usuario deje, serán reasignados por la UNIDAD DE ACTIVOS FIJOS en función a los requerimientos de la Institución. Para que el equipo permanezca en el área de trabajo original, la dirección o unidad respectiva deberá hacer llegar su solicitud a la UNIDAD DE ACTIVOS FIJOS

Unidad de Investigaciones Financieras Vo.Bo. C.I.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

10.4 LLENADO DE FORMULARIO DE SOLICITUD

El formulario de solicitud deberá contener como mínimo los siguientes datos:

a) Datos Personales
- Nombre del Empleado
- Dirección / Unidad
- Función o Cargo del Empleado
- Cuentas(s) Solicitada (s): debe marcar las opciones que solicita y tachar las restantes.

b) Datos de Autorización (llenado por el Jefe Unidad o Director del área solicitante):
- Fecha
- Nombre y cargo
- Firma y sello

c) Datos de Recepción, rechazo o aceptación (Completa la Jefatura de la JSTI)
- Fecha
- Nombre del responsable
- Firma y Sello

Para solicitudes de alta se deberá completar todos los datos, en caso de solicitudes de modificaciones se completará únicamente los datos de identificación a los datos sujetos de modificación, en caso de bajas, es suficiente completar los datos de la parte de datos de identificación.

Se completará un formulario por cada funcionario. Las solicitudes de alta y modificaciones deben llevar la firma del funcionario, y las solicitudes de baja se admitirá sin la firma del funcionario.

El funcionario autorizador es responsable de validar que las opciones no autorizadas estén tachadas antes de firmar o en su defecto hacerlo al momento de firmar. La jefatura de la JSTI asumirá como validas las opciones seleccionadas y no tachadas, sin embargo cuando lo crea pertinente podrá confirmar o rechazar la solicitud explicando al usuario solicitante y/o funcionario autorizador el motivo.

10.5 COMUNICACIÓN OPORTUNA

La comunicación de los movimientos de cuentas de usuario será realizada a la JSTI y deberá realizarse como mínimo con un día de anticipación.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

10.6 BLOQUEO DE USUARIOS

El área de Recursos humanos o la unidad correspondiente deberá solicitar el bloqueo temporal del usuario que por cualquier motivo se ausenten de su fuente de trabajo (vacaciones, licencias,

Unidad de Investigaciones Financieras Vo.Bo. J.J.C.G. JSTI

permisos, viajes u otra excusa) por más de cinco días laborales, para que la JSTI proceda a bloquear sus accesos durante un tiempo determinado.

10.7 IDENTIFICACION DE USUARIOS

Todo funcionario de la UIF debe tener un único nombre de usuario con el que será identificado, reconocido, autentificado y registrado en todos los sistemas informáticos de la UIF si es técnicamente posible. (Ver la sección Criterios Nominales de creación de cuentas personales en el capítulo de Uso de Correo Electrónico).

La existencia de usuarios genéricos debe ser solicitada a través de la plataforma de atención al usuario y autorizada por la JSTI. El/La Oficial de Seguridad realizara revisiones periódicas sobre la existencia de usuarios genéricos.

Los equipos de computación deberán contar un nombre o descripción independiente del nombre de usuario o la unidad.

11. INFORMACION

11.1. CUSTODIA DE LA INFORMACION

El personal de la JSTI, debe mantener en estricta custodia la información sensible asociada directa e indirectamente a la presente norma. Toda la información es considerada confidencial salvo se exprese lo contrario.

11.2. TRATAMIENTO DE INFORMACION

La información impresa relacionada con la presente normativa, deberá ser conservada durante doce meses, al cabo de los cuales podrá ser entregada a la unidad de archivo bajo inventario.

12. CONTROL DE SEGURIDAD

Todos los funcionarios deberán velar por el estricto cumplimiento de la presente normativa, siendo su responsabilidad denunciar cualquier sospecha o incumplimiento de violación a lo establecido ante el/la Oficial de Seguridad o la JSTI y procurar su aclaración en un tiempo prudente.

13. AREAS INVOLUCRADAS

Las áreas involucradas en la presente norma, son:

RECURSOS HUMANOS

- En la oportuna solicitud de alta, cambio o baja de cuentas a usuarios.

PERSONAL DE LA JSTI

- Generar los reportes definidos en la sección reportes del presente capítulo.

Unidad de Investigaciones Financieras Vo.Bo. C.L.G. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

- En el cumplimiento de las presentes disposiciones
- El adecuado soporte y colaboración a los usuarios.
- La administración y configuración de los dispositivos entregados a los usuarios.
- La administración de usuarios para sistemas, ambientes y servicios: alta, modificación de roles o privilegios, bloqueo y baja.

USUARIOS

- La oportuna solicitud de autorización para acceso y uso de los recursos tecnológicos de la UIF
- El adecuado custodio de los recursos entregados.
- En la preservación de la configuración física y lógica de los dispositivos recibidos.
- En el custodio y protección estricta de sus contraseñas o claves de acceso.
- En el estricto cumplimiento de la presente normativa.

14. INCUMPLIMIENTO Y SANCIONES

El incumplimiento de la presente norma será sancionado de acuerdo al Reglamento Interno de la UIF referente a las Infracciones y Sanciones.

CAPITULO VII - USO DE CORREO ELECTRONICO

1. OBJETIVO

La presente norma tiene como objetivo reglamentar el uso del correo electrónico institucional.

2. ALCANCE

Esta norma debe ser cumplida por todos los funcionarios de la UIF, consultores y personas que trabajan con una cuenta de correo electrónico asignada por la UIF.

3. DEFINICIONES PRINCIPALES

3.1 PROPIEDAD DE LA INFORMACION EN EL CORREO ELECTRONICO

Se considera de propiedad de la UIF todos los datos, documentos e información generados, haciendo uso de su plataforma informática, computadores personales y software, así como aquella que se genera por efecto de acciones de consulta, certificación o trabajo interactivo con usuarios internos y externos a través del portal, con excepción de la correspondencia personal que pudieran generar los usuarios internos de la red informática de la UIF.

3.2 MONITOREO Y CONTROL DE SEGURIDAD

Siendo los medios, canales y dispositivos utilizados para la explotación del correo electrónico, propiedad de la UIF, este se revela al derecho de auditar, monitorear , restringir , eliminar o implantar cualquier medida de seguridad para proteger la información que circula a través de el.

3.3 USO DEL CORRERO ELECTRONICO

El servicio de correo electrónico debe ser utilizado para fines institucionales. Este podrá ser utilizado para fines personales de una manera razonable y controlada siempre y cuando no perjudique los procesos de la UIF.

El/La Oficial de Seguridad pondrá a consideración de la JSTI anualmente los parámetros para considerar el uso de este servicio como razonable o no perjudicial para la UIF. No esta permitido el acceso a otro tipo de correo electrónico vía web (Hotmail, yahoo, email o similares) de ningún funcionario, a menos que la JSTI autorice el acceso en casos de emergencia.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

3.4 PROTECCIÓN DEL CORREO ELECTRONICO

La JSTI es responsable de:

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

- Los niveles de seguridad en los diferentes canales de comunicación utilizados por este servicio que garanticen la confidencialidad, integridad y disponibilidad del mismo.
- Los medios de retención y almacenamiento de la información relacionada mientras se encuentren centralizados.
- La administración de cuentas usuarias: altas, modificaciones y bajas.

3.5 RESPONSABILIDAD SOBRE EL CONTENIDO DEL CORREO ELECTRONICO

El correo electrónico es designado canal oficial únicamente para comunicaciones internas. Al ser este un medio de transmisión de información confidencial, esta certificado como un medio seguro de transmisión por la JSTI.

Queda prohibido el envío de información confidencial fuera de la institución salvo autorizaciones estrictas de la Dirección o Unidad correspondiente (titulares de la información), teniendo el funcionario la responsabilidad por la información enviada.

La información que no requiera autorización para ser transmitida, incluyendo la información personal, es de enterar responsabilidad del titular, quedando la Institución libre de la responsabilidad que implica el contenido de la misma.

- Si el mensaje es Externo: Debe contener al menos: Nombre, Cargo, Unidad o Area, Dirección, Institución y URL. Por ejemplo:

Juan Pérez V.
Responsable de Unidad
Jefatura de Sistemas y Tecnologias de la Informacion
Unidad de Investigaciones Financieras
Calle Loayza, No 155
www.uif.gob.bo

Si es interino debe contener al menos Nombre y el teléfono interno del remitente.

- Declaración institucional, El pie de página en todos los mensajes debe contener de forma automática la siguiente declaración:

********** FAVOR TOMAR NOTA **********
Este mensaje, y cualquier archivo adjunto, puede ser confidencial o legalmente privilegiado. El mismo ha sido concebido solo para las personas nombradas quienes son los únicos destinatarios autorizados. Si este mensaje le ha llegado por error, sea tan amable de eliminarlo sin revisarlo y notifique al remitente inmediatamente.
Gracias por su ayuda
****

Si el usuario detectase que no está generando este pie de correo debe informarlo al JSTI.

4. ADMINISTRACION

4.1 ADMINISTRACION DE CUENTAS DE CORREO ELECTRONICO

Unidad de Investigaciones Financieras Vo.Bo. C.U.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

La UIF gestiona las cuentas de correo electrónico en el dominio @uif.gob.bo bajo este dominio, se distinguen tres tipos de cuentas: personales, grupales y genéricas.

Las cuentas personales se ajustarán a lo expuesto en la sección 5.2 (Criterios nominales de creación de cuentas personales). Para disponer de una cuenta personal de correo electrónico, el usuario deberá tener una relación laboral con la UIF.

En el caso de funcionarios de la UIF, éstas serán asignadas en función del cargo que ocupa la persona, pudiendo existir algunos que por su naturaleza no requieren de una cuenta de correo o que solamente requieran correo interno, este caso será determinado por las diferentes unidades.

Las cuentas grupales son administradas por la jefatura de la JSTI en cuanto a la creación, adición o eliminación de componentes. Deberá ser solicitada e indicando sus componentes y vigencia.

La gestión de estas cuentas debe estar respaldada por un formulario impreso (ver formulario de solicitud (ver anexos), y firmado por el responsable de la solicitud y la dirección correspondiente.

CRITERIOS DE CREACION DE CUENTAS PERSONALES

La forma común de una cuenta de correo electrónico es:

Alias del_usuario@domino.com
En la UIF, el alias_del_usuario se construye utilizando las siguientes estructuras:

- primer nombre.primer apellido (separados por un punto) que es el criterio preferente.
- Primer nombre y segundo nombre.primer apellido
- Primer nombre.primer apellido y segundo apellido

CUENTAS GENERICAS

La creación de una cuenta genérica esta restringida a las Dirección, Unidades y Servicios de la UIF y deberán satisfacer los siguientes criterios:

- En casos de nombres compuestos como estructura y procesos se podrá colocar abreviaciones compuestas separadas por punto o no. Por ejemplo: estrucura.proceso@domino.com

Para la creación de cuentas genéricas se debe efectuar la misma solicitud que para las cuentas personales. Es necesario indicar la duración prevista de la cuenta y la persona responsable.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

CUENTAS GRUPALES

- Debe prevalecer el principio de asociación simple entre el alias de la cuenta y el grupo asociado, por ejemplo: direcciónde sistemas@uif.gob.bo.

En todos los casos se deberá:

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

- Los caracteres con tilde son sustituidos por el mismo carácter sin tilde. El carácter ñ es sustituido por la letra n.
- En caso de combinaciones que deriven en palabras no adecuadas o incomodas podrá solicitarse el cambio de identificador de usuario.
- En apellidos compuestos se eliminan los espacios.

CUENTAS PERSONALES PARA PASANTES UNIVERSITARIOS (SI CORRESPONDIERA)

En este caso se creara una cuenta temporal para que el usuario tenga acceso a la red, pero no contara con uso de correo electrónico. La cuenta estará identificada con la siguiente estructura:

- p. (separado por un punto) primer nombre. (punto) primer apellido que es el criterio preferente, ejemplo: p.nombre.primerapellido@uif.gob.bo

DESACTIVACION DE CUENTAS DE CORREO

Las cuentas deben desactivarse en los siguientes casos:

- cuentas genéricas o grupales: cuando se alcance su periodo de caducidad.
- Cuentas personales (naturales y/o jurídicas): cuando la Unidad de Recursos Humanos o el área responsable comunique la finalización de la relación contractual del usuario con la UIF.

El uso inapropiado o el abuso del servicio de correo electrónico ocasionará la desviación temporal o permanente de las cuentas. Las acciones en este sentido pueden llevarse a cabo en función de las incidencias que puedan causar un problema para el buen funcionamiento del servicio.

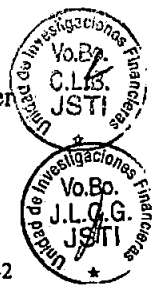
RESPECTO A LAS LEYES DE PRIVACIDAD

Excepto el personal de la JSTI específicamente autorizado y designado para la administración y control del correo electrónico, al resto de los funcionarios de la UIF.

5. DE LA LISTA DE ARCHIVOS AUTORIZADOS

La lista de archivos autorizados para su envió mediante correo electrónico (interno/externo), de acuerdo a su extensión será la siguiente:

- Documentos con extensión *.doc, *.txt, *.rtf, *.pdf, *.htm, *.html, *.dot, *.xml.
- Hojas electrónicas con extensión *.xls, *.xlt, *.csv.
- Presentaciones con extensión: *.ppt, excepto las que no contengan información de carácter relacionado al trabajo de la UIF.
- Archivos comprimidos con extensión: *.zip, *.rar .
- Archivos de imágenes con extensiones preferentemente *.jpg, *.gif, *.tif, *.bmp.
- Archivos de planos con extensión: *.dwg, *.dxf.



El/La Oficial de Seguridad y/o la JSTI son los responsables de autorizar nuevas extensiones de archivos autorizados.

6. DEL USO DEL CORREO

6.1 RESPONSABILIDADES DE LOS USUARIOS CON RESPECTO AL USO DEL CORREO ELECTRONICO

No esta permitido utilizar el correo electrónico para:

- Enviar mensajes cadena, Junk mail, correo Chatarra (mensajes de Amistad, confraternidad, presentaciones, gráficos, etc.), correo no solicitado (spam mail) o cualquiera que tenga características similares.
- Difamar, abusar, desacreditar, acosar, amenazar o violar los derechos (tales como derechos de privacidad) de otros.
- Participar de manera directa o indirecta en negocios con fines económicos personales.
- Publicar, distribuir o exhibir material o información difamatoria, obscena, indecente, pornográfica o ilegal que pueda o no tener consecuencias legales.
- Coleccionar o recoger información de otras personas, incluyendo direcciones de correo electrónico sin previo consentimiento.
- Engañar a terceros representando una falsa identidad de rendimiento de remitente o del origen de un mensaje.
- Suscribirse a listas públicas u otras sin fines institucionales.
- Adjuntar cualquier material / información que contenga virus: troyanos, gusanos, bombas de tiempo, cualesquiera otro programa dañinos o peligroso o que no esté en la lista de archivos autorizados para envió por correo electrónico.
- Adjuntar cualquier material que contenga software u otro material protegido por derechos de autor, propiedad intelectual, derechos de privacidad o cualquiera otra ley aplicable.
- Intentar acceder de manera no autorizada a otras cuentas de correo electrónico.
- Facilitar información de la UIF a otros individuos, compañías u organizaciones, sin autorización formal de la dirección y/o unidad respectiva.
- Enviar mensajes con firmas escaneadas para dar la impresión que el remitente firma un mensaje del correo electrónico.
- Enviar mensajes con archivos adjuntos mayores a 5 mega Bytes (MB). Para enviar Mensajes de mayor tamaño se recomienda particionar o comprimir dichos adjuntos.
- Adjuntar archivos de tipos no autorizados por la JSTI (exe, scr, reg y otros) los mismos que pueden ser eliminados del mensaje por la JSTI.

6.2 ADMINISTRACION DEL ARCHIVO BASE
ARCHIVO BASE EN ELSERVIDOR DE CORREO ELECTRONICO

Cuando los datos usuarios asociados al correo electrónico residen en el servidor como copia o archivo único, la JSTI es responsable de:

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.I.C.G. JSTI

- Establecer cuotas o espacios mínimos por niveles jerárquicos que limiten el tamaño de estos archivos.
- Definir medidas de seguridad para optimizar la disponibilidad de los datos y del servicio mediante la ejecución de respaldos periódicos, uso de herramientas antivirus y otras medidas que considere necesarias.

ARCHIVO BASE EN EL PC DEL USUARIO

Cuando los datos usuarios asociados al correo electrónico residan en el PC del usuario como copia o archivo único, el usuario es responsable de:

- Verificar y controlar periódicamente el tamaño del archivo base almacenado en su equipo para que este no alcance tamaños muy grandes que puedan poner en riesgo su uso el mismo que no puede exceder los 1.5 giga bytes.
- Solicitar la realización de copias de respaldo de sus archivos base.

6.3 ACCESO REMOTO

La habilitación de acceso remoto a las cuentas de correo electrónico solo esta autorizado para el personal ejecutivo de la UIF.

6.4 ABUSOS DEL CORREO ELECTRONICO

Determinadas prácticas en el uso de la cuenta de correo electrónico están catalogadas como abuso del Correo Electrónico. Estas actividades están prohibidas en la UIF y los abusos de correo pueden agruparse en categorías las mismas que serán:

- Difusión de contenido inadecuado: Contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos). Ejemplos: programas piratas, amenazas, estafas, virus o código malicioso.
- Difusión a través de canales no autorizados: uso no autorizado de cuenta ajena para reenviar correo propio. Aunque el mensaje en si sea legitimo, se esta utilizando recursos ajenos sin su consentimiento.
- Difusión masiva no autorizada: el uso de cuentas propias o ajenas para enviar masivamente mensajes de correo no solicitados por el destinatario, sean o no publicitarios, no esta permitido.
- Ataques con objeto de imposibilitar o dificultar el servicio de correo electrónico: Pueden dirigirse a un usuario o al propio sistema de correo. En ambos casos, el ataque consiste en envió de un numero alto de mensajes por segundo, o cualquier variante, que tenga el objetivo de paralizar el servicio por saturación de las líneas, la capacidad de CPU del servidor, o el espacio en disco de servidor o usuario.

La responsabilidad de esta tipo de abuso puede ser tanto por acción como por omisión, pues existe gran cantidad de software que genera mensajes de correo electrónico automáticamente y que con una configuración inapropiada pueda suponer una merma en la calidad del servicio general.

6.5 GARANTIA DE ENTREGA

Aunque en un porcentaje muy elevado de los casos, los mensajes de correo electrónico llegan a su destino rápidamente, en ningún caso el servicio de correo electrónico y la JSTI garantizan la entrega de un mensaje. Numerosas circunstancias pueden impedir la recepción de un mensaje: caídas imprevistas en las líneas de rechazo de mensajes por virus, exceso de tamaño para el servidor que recibe, direcciones mal formadas y otros.

Por estos motivos no existe una garantía 100% certera de la entrega de un correo a su destinatario, debiendo el usuario remitente tomar las precauciones adecuadas para validar la recepción de un correo electrónico.

6.6 SERVICIOS NO ESTANDAR RELACIONADOS CON EL CORREO ELECTRONICO

AUTO RESPONDEDORES

El servicio de correo de la UIF no permite definir auto respuesta de correos electrónicos.

6.7 PROTECION DE ANTIVIRUS.

Algunos archivos adjuntos pueden contener peligrosos virus que dañarían los recursos de la UIF. Los usuarios nuca deberán aceptar correos electrónicos con documentos adjuntos enviados externamente, sin que previamente el material sea revisado por el antivirus institucional. Si el usuario sospecha sobre la existencia de un virus debe notificar al encargado de plataforma de atención al cliente.

La JSTI NO pide a los beneficiarios de una cuenta de correo, en el dominio @uif.gob.bo, la confirmación de cuentas y sus contraseñas (passwords) a través de formularios electrónicos, la recepción de este tipo de correos debe ser denunciada a la JSTI.

7. DE LA INFORMACION

7.1 CUSTODIA DE LA INFORMACION

El personal de la JSTI, debe mantener en estricta custodia la información sensible asociada directa e indirectamente a la presente norma. Toda la información es considerada confidencial salvo se exprese lo contrario.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

7.2 TRATAMIENTO DE INFORMACION SENSIBLE

La información impresa relacionada con la presente normativa, deberá ser conservada durante 12 meses, al cabo de los cuales deberá ser entregada a la unidad de archivo bajo inventario.

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

8. DEL CONTROL

8.1 CONTROL DE SEGURIDAD

Todo el personal de la UIF debe velar por el correcto uso del servicio de correo electrónico, debiendo denunciar cualquier uso indebido, apropiación de identidad electrónica, acceso a información sensible y cualquier sospecha de incidente o violación de la seguridad, al Oficial de Seguridad o mediante Soporte a Usuarios.

9. AREAS INVOLUCRADAS

Las áreas involucradas en la presente norma, son:

PERSONAL DE LA JSTI

- En la supervisión y definición de los niveles de servicio del correo electrónico.
- En la supervisión del incumplimiento de la presente norma.
- En la autorización para la creación de cuentas de correo de personal interno o para grupos de usuarios.
- En la administración de los recursos tecnológicos relacionados con este servicio.
- En la definición de cuotas para usuarios.
- En la generación de reportes gerenciales.
- Generar los reportes definidos en la sección reportes del presente capitulo.
- En el cumplimiento de las presentes disposiciones.

OFICIAL DE SEGURIDAD

- En la revisiones de cumplimiento de la presente normativa.
- En la revisión de administración de cuentas vigentes, vencidas, eliminadas.
- En la acreditación del entorno de seguridad del servicio de correo electrónico.

USUARIOS FINALES

- En el adecuado uso y explotación del servicio de correo electrónico según las presentes disposiciones.
- En la administración de sus archivos base de correo cuando estos residen en su PC
- En la protección de su cuenta de correo electrónico.

10. INCUMPLIMIENTO Y SANCIONES

El incumplimiento a la presente norma será sancionado de acuerdo al reglamento Interno de la UIF referente a Infracciones y sanciones.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

CAPITULO VIII - GESTIÓN DE COMUNICACIONES

1. OBJETIVO

La presente norma tiene como objetivo reglamentar la administración de servicios de la red de Comunicaciones, establecer los procesos y actividades administrativas relacionadas como la planificación, configuración, control, monitoreo de los elementos que conforman una red, con el fin de asegurar el eficiente y efectivo empleo de sus recursos, lo cual se vera reflejado en la calidad de los servicios ofrecidos más importantes.

Se considera la administración de las líneas tanto externas (telecomunicación), como internas (redes) de todos los dispositivos conectados a la red local.

2. ALCANCE

La presente norma debe ser aplicada por todos los funcionarios de la JSTI, funcionarios y personas que tienen relación con la UIF que utilizan la red.

3. EQUIPOS DE COMUNICACIÓN

La jefatura de la UIF es responsable de los equipos de comunicación ubicados en las oficinas de la UIF, en lo que se refiere al mantenimiento, cuidado y buena utilización, así como de su ubicación en lugares adecuadamente ventilados, seguros y estables.

Los dispositivos físicos deben estar estrechamente asociados con las recomendaciones del proveedor o fabricante de los dispositivos, por ellos se hace necesario contar con los manuales técnicos actualizados y disponibles para su consulta. Esta actividad está bajo responsabilidad del encargado de redes y comunicaciones quien deberá recolectar estos documentos y entregarlos bajo inventario a la jefatura de la JSTI. Esta documentación podrá ser en formato electrónico

4. ADMINISTRACIÓN DE RECURSOS TECNOLÓGICOS

4.1 ALTA DE DISPOSITIVOS

Cuando un dispositivo de red es entregado para su explotación a la Jefatura de la JSTI, esta debe dar de alta al mismo en coordinación con la Unidad de Activos Fijos, como parte del inventario de recursos tecnológicos disponibles para su explotación asignado un código para su identificación.

El Encargado de Redes y Comunicación debe probar el normal funcionamiento del dispositivo al momento de su aceptación o recepción y ejecutar las herramientas disponibles de los dispositivos y extraer las características técnicas las mismas que serán registradas por el Área de Activos de la UIF.

4.2. MANTENIMIENTO DE DISPOSITIVOS

La jefatura de la JSTI es responsable de realizar la planificación y ejecución del mantenimiento en coordinación con el (los) Encargado (s) de Redes y Comunicación, tanto en la oficina central como en las Departamentales.

4.3. MANTENIENDO PREVENTIVO

El encargado de Redes es responsable de la planificación y ejecución del mantenimiento preventivo, y también de supervisar el cumplimiento si el mantenimiento es externo (servicio realizado por una empresa).

Cuando el mantenimiento preventivo es realizado por un proveedor externo, el encargado de Redes es Responsable de Supervisar y revisar después del mantenimiento la configuración del dispositivo de red, tanto de hardware como de software.

4.4. MANTENIMIENTO CORRECTIVO

El encargado de Redes y Comunicaciones es responsable de realizar o supervisar el mantenimiento correctivo cuando ocurra un daño o falla imprevista de un dispositivo de red.

4.5. MOVIMIENTO DE DISPOSITIVOS

Todo movimiento de dispositivos debe ser realizado bajo supervisión y responsabilidad del Encargado de Redes y Comunicaciones por la sensibilidad y conocimiento técnico requerido. Todo movimiento de dispositivos de comunicación debe ser coordinado y comunicado con El Area de de ACTIVOS FIJOS.

4.6. INSTALACIÓN FÍSICA Y CONFIGURACIÓN LÓGICA DEL DISPOSITIVO

El encargado de Redes y Comunicaciones deberá realizar o supervisar la instalación física y la configuración lógica del dispositivo de red de acuerdo al manual técnico del mismo, previa autorización de la jefatura de la JSTI.

5. ADMINISTRACION DE FALLAS

5.1. MONITOREO Y CONTROL

El encargado de Redes y Comunicación es responsable de monitorear el cumplimiento de las cláusulas establecidas en el contrato cuando el mantenimiento es cumplido por un tercero.

Cuando el encargado de Redes y Comunicación de la UIF es la responsable del monitoreo y control, esta debe contar con un sistema de monitoreo de alarmas (automático o manual) por ejemplo alarmas de instrucción, de sobrecarga, de conexión de nodos o disponibilidad y otras para identificar si existe un problema en la red y procurar su disponibilidad continua.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

5.2. TIPOS DE FALLA

El encargado de Redes y Comunicaciones es responsable de la detección y resolución oportuna de situaciones anormales en los dispositivos de red.

FALLA PERMANENTE

El encargado de Redes y Comunicaciones deberá verificar si existe la garantía del dispositivo o si está incluida en el contrato de mantenimiento correctivo su reposición y/o reparación.

FALLA TEMPORAL

El encargado de Redes y Comunicaciones es responsable de solucionar o supervisar el arreglo de la falla temporal del dispositivo.

5.3. FALLA EN EQUIPOS CRÍTICOS

El encargado de Redes y Comunicaciones deberá, estimar el impacto de servicios afectados por la falta en los equipos críticos y comunicaciones con la jefatura de la JSTI y/o los responsables de los procesos afectados para dar prioridad a su recuperación.

5.4. CAMBIO CON EQUIPOS PRESTADOS

El encargado de Redes y Comunicaciones deberá ser el responsable de la prueba de funcionamiento, instalación y custodia del dispositivo prestado hasta su devolución. Deberá mantener un registro o ficha técnica del dispositivo.

6. ADMINISTRACION DE CLAVES

6.1. RESPONSABILIDAD DE LA CLAVE DE CONFIGURACIÓN

La clave de configuración de todos los equipos de comunicación de la UIF es responsabilidad del encargado de Redes y Comunicaciones.

6.2 ALMACENAMIENTO DE LA CLAVE DE CONFIGURACIÓN

El encargado de Redes y Comunicaciones tendrá registradas todas las claves de los equipos de comunicaciones de forma impresa, en el Telkey a cargo del Oficial de Seguridad ubicado en la JSTI, estas claves se actualizaran de acuerdo a normativa.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

6.3. CAMBIO DE LA CLAVE DE CONFIGURACIÓN

En caso de cambio de claves, se procederá a informar el jefe de la JSTI a través del encargado de Redes y Comunicaciones, en cumplimiento a la normativa de custodia de Claves de Información y Tecnología.

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

7. CONFIGURACION Y CAMBIOS

7.1. AUTORIZACIÓN DE CAMBIOS Y CONFIGURACIÓN

Para todo cambio, actualización y configuración de hardware de los equipos y líneas de comunicación el responsable solicitara la autorización respectiva el encargado de Redes y Comunicaciones. Cuando los cambios sean de emergencia se deberá proceder según norma y procedimientos de Administración de Problemas e incidentes.

7.2. REGISTRO DE CAMBIOS DE CONFIGURACIÓN

El encargado de Redes y Comunicaciones mantendrá una carpeta con documentación impresa sobre la configuración de la red, la configuración de los equipos de comunicación y los trabajos en curso.

Una copia de esta carpeta la almacenara el jefe de la JSTI, para efectos de ejecución del plan de contingencia, siendo responsabilidad del encargado de Redes y Comunicaciones informar y proveer de actualizaciones impresas de esta documentación, cada que se produzca un cambio. En todo momento ambas carpetas deberán contar con la información actualizada.

7.3. BITÁCORA DE COMUNICACIONES

El encargado de Redes y Comunicaciones coordinara con los operadores el llenado diario de la bitácora de comunicaciones y/o novedades, que debe contener al menos fecha y hora, descripción del incidente, solución y observaciones.

7.4. ADMINISTRACIÓN DE LAS DIRECCIONES IP

El encargado de Redes y Comunicaciones es el responsable de la administración adecuada de las direcciones IP.

Se reservara direcciones IP para equipos críticos como Servidores, enrutadores, impresoras y otros.

Se mantendrá un registro de las direcciones IP asignadas por usuario y dispositivo.

8. CONTROL DE SEGURIDAD

8.1. SEGURIDAD

El encargado de Redes y Comunicaciones es responsable por la seguridad lógica y física de los dispositivos de red y comunicaciones. Su responsabilidad se extiende hasta la solicitud formal de los medios y recursos preventivos para garantizar la seguridad lógica y física.

Deberá crear estrategias para la prevención de ataques, detección de intrusos, respuesta a incidentes que atenten contra la seguridad y proponerla al jefe de la JSTI, para su autorización e implementación.

8.2 HERRAMIENTA DE SEGURIDAD

Ningún funcionario de la UIF deberá instalar o hacer uso de este tipo de herramientas sin contar con la debida autorización del encargado de Redes y Comunicaciones.

Encargado de Redes y Comunicaciones podrá auxiliarse de herramientas de seguridad como IDS, sistemas de escaneo de puertos y otros.

El encargado de Redes y Comunicaciones deberá solicitar el permiso de uso de estas herramientas al jefe de la JSTI.

9. ADMINISTRACION DE LA RED

9.1. ADMINISTRACIÓN DE LA CONFIGURACIÓN

El encargado de Redes y Comunicaciones deberá satisfacer los requerimientos inmediatos y futuros de la red, y reflejamos en su diseño hasta llegar a su autorización e implementación. Debe seleccionar la infraestructura de la red de acuerdo a las necesidades y la topología aprobada.

El encargado de Redes y Comunicaciones es responsable de la instalación de hardware de red. Toda instalación deberá realizarse bajo su supervisión u autorización. Es responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además deberá mantener un control sobre los programas que son creados para obtener información específica en los dispositivos.

9.2. ADMINISTRACIÓN DEL RENDIMIENTO.

El encargado de Redes y Comunicaciones podrá observar y recolectar la información referente al comportamiento y características del tráfico que circula por la red. El encargado de Redes y Comunicaciones deberá interpretar la información monitoreada, determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño. Deberá detectar comportamientos relacionados como:

- Trafico inusual de la información
- Caídas, cortes, saturaciones de los elementos principales de la red.
- Calidad de servicio
- Otros

El encargado de Redes y Comunicaciones debe identificar la obsolescencia tecnológica de los dispositivos de red e informar a Jefatura de la JSTI cuando considere a un dispositivo obsoleto

9.3. DISPONIBILIDAD

El encargado de Redes y Comunicaciones es el responsable de supervisar la disponibilidad de los recursos necesarios para que la red funcione y pueda ser monitoreada bajo las normativas definidas y deberá comunicar al jefe de la JSTI la necesidad de disponer de Recursos faltantes.

10. INFORMACION

10.1. CUSTODIA DE LA INFORMACIÓN

Todos los funcionarios de la JSTI, debe mantener en estricta custodia la información sensible asociada directa e indirectamente a la presente norma. Toda información es confidencial salvo se exprese lo contrario.

10.2. TRATAMIENTO DE LA INFORMACIÓN SENSIBLE

La información impresa relacionada con la presente normativa, deberá ser conservada durante 12 meses, al cabo de los cuales podrá ser entregada a la unidad de archivo bajo inventario.

11. CONTROL DE SEGURIDAD

Todas las funciones del encargado de Redes y Comunicaciones asociadas a telecomunicaciones y redes deben ser aprobadas y documentadas para control. Las funciones de control se refieren específicamente a:

- Uso de los recursos
- Seguridad de los accesos (pruebas de intrusión)
- Medición de calidad de atención al usuario.
- Mantenimiento actualizado del inventario de recursos
- Mantenimiento y control de la configuración establecida
- Realización del mantenimiento preventivo y correctivo.
- Mantenimiento de guías y manuales usuarios.

12. AREAS INVOLUCRADAS

Las áreas involucradas en la presente norma son:

EL ENCARGADO DE REDES Y COMUNICACIONES

- En la ejecución de los procedimientos según las disposiciones del presente documento.
- En el cumplimiento de la presente normativa.
- En el adecuado resguardo de los informes con claves actualizadas.
- En la coordinación con el jefe de la JSTI y Tecnología todas las actividades que involucren la administración de recursos tecnológicos telecomunicaciones y redes.

USUARIOS FINALES

- En el adecuado uso y explotación de la red de comunicaciones de la UIF
- La oportuna solicitud de autorización para acceso y uso de los recursos tecnológicos de la UIF
- En el estricto cumplimiento de la presente normativa

13. INCUMPLIMIENTO Y SANCIONES

En el incumplimiento a la presente norma será sancionado de acuerdo al Reglamento Interno de la UIF en Infracciones y Sanciones

CAPITULO IX - ADMINISTRACIÓN DE PROBLEMAS E INCIDENTES

1. OBJETIVO

La presente norma tiene por objetivo controlar todo el problema e incidente que se presente en los sistemas de información de la UIF a fin de tener mejores niveles de continuidad de procesamiento y alta disponibilidad en los ambientes de Información y Tecnología, parámetros de sistema, procedimientos operativos, hardware y software, facilidades entre otros.

2. ALCANCE

La administración de Problemas e Incidentes, permita actuar de inmediato ante una situación de emergencia materializada en cualquiera de las dependencias de la JSTI de la UIF. Con este antecedente, la presente norma será aplicable a todos los Niveles: Direcciones Departamentales, Jefaturas de Unidades, Funcionarios de la institución, los cuales en su trabajo utilizan recursos tecnológicos pertenecientes a la UIF, pudiendo detectar y/o experimentar problemas en el cumplimiento de sus funciones, con el uso de los recursos mencionados. El presente procedimiento, con el uso de los recursos mencionados. El presente procedimiento se aplicara hacia el interior de la UIF.

La presente norma incluye a todo los funcionarios de la UIF en la atención y solución de los problemas e incidentes.

3. REGISTRO DE PROBLEMAS

Toda detección de un problema o incidente de magnitud identificado por los usuarios o funcionario de la UIF debe ser canalizado por Jefatura de la JSTI. Si este no esta disponible y el incidente o problema es crítico, el registro podrá hacerse de manera posterior por el responsable de la solución del problema o incidente.

Todos los usuarios de los sistemas de información son responsables de denunciar un hecho ocurrido o que tiene la potencialidad de ocurrir, debiendo registrar su denuncia con el/la Oficial de Seguridad. Se considera esta la vía formal para denunciar potenciales incidentes que puedan afectar la información o activos de la UIF y queda prohibido propagar la denuncia por canales no autorizados.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

4. ARCHIVOS DE INCIDENCIA

Para la Administración de Problemas e Incidentes se dispondrá de una lugar físico donde se pueda guardar toda la información relacionada a los incidentes ocurridos y con acceso exclusivo de la Jefatura de la JSTI. Toda la documentación adjunta será almacenada en orden cronológico de ocurrencia del incidente o problema. Se debe dividir del archivo de documentos por el tipo de incidencia por ejemplo:

- Archivo de incidencias de hardware.

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

- Archivo de incidencias de software

5. DE LOS PROBLEMAS E INCIDENTES

5.1. DEFINICIÓN DE PROBLEMAS E INCIDENTES

El/la Oficial de Seguridad deberá definir una clasificación de los problemas e incidentes por su naturaleza y deberá tipificarlos, por ejemplo agrupados por hardware, software y facilidades. Esta clasificación debe ser revisada como mínimo anualmente.

5.2. ATENCIÓN DE PROBLEMAS O INCIDENTES EN PRODUCCIÓN (RIESGO/IMPACTO)

El/la Oficial de Seguridad para la solución del problema o incidente debe evaluar el riesgo/impacto del problema o incidente en una escala simple de: alto, medio y bajo. Riesgo/Impacto puede presentarse en términos:

- Económicos: Disminución directa de los ingresos, incremento de los gastos, erogaciones innecesarias o no justificadas.
- Patrimoniales: Daño de los recursos de información y tecnología.
- Productivos: Tiempo perdido hasta el re-inicio de las actividades.
- De servicio a los clientes: Calidad disminuida por paros en la atención de clientes internos y externos
- Normativos: incumplimiento de normativas internas o externas relacionadas.
- De desarrollo institucional: Limitantes en el crecimiento, obstáculos y público en general.
- Legales: Incumplimiento de Normas Legales.
- Operativo/Administrativo: Aplicación de procedimientos alternativos que pueden alterar el normal funcionamiento de la institución. Por ejemplo, compras o pagos no planificados o presupuestados, no emisión de cheques.

EL/la Oficial de Seguridad deberá identificar medidas preventivas y comunicarlas a la comunidad de usuarios afectados además de registrarlo.

6. ESCALAMIENTO

El escalamiento de Problemas o Incidentes se debe efectuar cuando los responsables asignados, primer nivel, no puedan atender y resolver los mismos. El impedimento puede tener origen en la falta de conocimiento, falta de recursos tecnológicos, prioridad asignada o autorizaciones que pueden estar fuera del nivel asignado por la JSTI. Cuando se produzca esta situación, se deberá comunicar al encargado de plataforma de atención el usuario (soporte a usuarios). Si las condiciones mencionadas anteriormente no permiten solucionar el problema se escala a un nivel más alto (Analista, supervisor) , quien podrá coordinar con las Unidades y/o los titulares de la información quienes por el impacto y riesgo deberán considerar el escalamiento al nivel Ejecutivo.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

7. REINCIDENCIA O REPETICION

En caso de reincidencia o repetición del Problema o Incidente el/la Oficial de Seguridad de o el Encargado del proceso solicitado, debe recurrir en primera instancia a revisar los datos almacenados y registrados en los documentos que se asemejen al caso en curso.

El/la Oficial de Seguridad deberá recopilar los documentos de problemas e incidentes para posteriormente realizar un análisis minucioso y determinar el motivo o causa de la reincidencia o repetición del problema, para plantear soluciones o generar requerimientos para su solución definitiva.

8. DOCUMENTACION DE PROBLEMAS E INCIDENTES

Toda atención de un problema o incidente de magnitud deberá tener revisión independiente. Al finalizar la solución del problema o incidente el/la Oficial de Seguridad deberá documentar la ocurrencia adjuntando la documentación mínima indispensable para su "revisión posterior".

9. INFORMACION

9.1. CUSTODIA DE INFORMACIÓN

Todo funcionario de la JSTI, debe mantener en estricta custodia la información sensible asociada directa e indirectamente a la presente norma. Toda información es confidencial salvo se exprese lo contrario.

9.2 TRATAMIENTO DE INFORMACIÓN SENSIBLE

La información impresa relacionada con la presente normativa, deberá ser conservada durante 12 meses, al cabo de los cuales podrá ser entregada a la unidad de archivo bajo inventario.

La información en medios digitales quedara bajo resguardo de la JSTI sujetas a disposiciones legales en cuanto a término y plazos de custodia.

10. CONTROL

10.1. CONTROL DE SEGURIDAD

El proceso de Administración de Problemas e Incidentes de magnitud debe mantener todos los registros posibles para validar el cumplimiento del procedimiento en forma efectiva y eficiente.

El control se debe ejercer a cada nivel que está involucrado en la tarea, tanto como autocontrol, control interno o independiente.

11. AREAS INVOLUCRADAS

Las áreas involucradas en la presente norma son:

TITULAR DE LA INFORMACIÓN

- En la autorización de las soluciones planteadas por el responsable de la solución del problema cuando corresponda.
- En la verificación de las soluciones planteadas por le responsable de la solución del problema.

OFICIAL DE SEGURIDAD

- Responsable por la custodia físico de los registros de problemas e incidentes de magnitud.
- Responsable por la elaboración de los reportes gerenciales.

CLIENTE O USUARIO DE LOS SERVICIOS DE INFORMACIÓN

Todos los clientes o usuarios son responsables de denunciar un hecho ocurrido o que tiene la potencialidad de ocurrir, por los canales autorizados.

PERSONAL DE LA JSTI

- Evaluar y definir que situaciones deben ser informadas a Dirección General Ejecutiva.
- Velar por el cumplimiento de la presente norma.
- Mantenerse informado cuando se sospecha de un problema o incidente reportado.

12. INCUMPLIMIENTO Y SANCIONES

El incumplimiento a la presente norma será sancionada de acuerdo a Reglamento Interno de la UIF en "Infracciones y Sanciones".

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.L.G. JSTI

ANEXOS

ANEXO A - Estación de Trabajo

Para bloquear su estación de trabajo en Windows 2000 Professional Windows 7 y Windows XP:

- Presiones CTRL + ALT + DELETE, seguidamente aparecerá una ventana de seguridad.
- Realice un clic en la opción Bloquear Equipo. Su estación de trabajo se habrá bloqueado.

Para desbloquear su estación de trabajo:

- Presiones CTRL + ALT + DELETE seguidamente aparecerá una ventana de seguridad.
- Ingrese su contraseña y luego realice un clic en el botón OK.

Para configurar su protector de pantalla con contraseña:

- Realice un clic sobre INICIO
- Luego en CONIGURACION
- Realice un doble clic en el PANEL DE CONTROL
- Seleccione el icono de PANTALLA
- Realice un clic en la pestaña PROTECTOR DE PANTALLA, la cual activara una ventana.
- Asegúrese de que la opción protegido por contraseña este activada.
- Seguidamente en la opción de espera, ingrese cinco minutos.
- Realice un clic APLICAR
- Luego en ACEPTAR

Su protector de pantalla se activara automáticamente después de cinco minutos de inactividad.

ANEXO B - Accesos a Internet

	USUARIOS CON ACCESO A INTERNET
	Jefatura de sistemas y tecnologías de la información
Página: ___ de ___	

Nombre de Usuario	Cuenta de Dominio	Dirección / Jefatura	Tipo de Acceso					Autorizado por:
			1	2	3	4		
Realizado por:			Revisado por:					Fecha:

Unidad de Investigaciones Financieras Vo.Bo. C.L.G. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

ANEXO C FORMULARIO DE SOLICITUD DE INTERNET

UNIDAD DE INVESTIGACIONES FINANCIERAS		
UIF BOLIVIA	FORMULARIO DE SOLICITUD DE ACCESO A INTERNET	VERSION: JSTI-V.1-2013

Nombre:		**Fecha Solicitud:**	
Área:		**Fecha de Inicio:**	

Por razones de seguridad la presente solicitud tiene validez hasta las fechas de corte trimestrales, a fines de Marzo, Junio, Septiembre, Diciembre, exceptuando Jefes de Unidad y Dirección

Páginas a Visitar:

Justificación:

Observaciones:

Firma Solicitante	**Firma Visto Bueno Jefe de Área (Solicitante)**	**Firma Dirección UIF**

CONDICIONES DE USO DE LA CONEXIÓN DE A INTERNET

1. La conexión a internet de la UIF es una herramienta de trabajo y no debe ser utilizada para fines personales o ajenos a los objetivos de la Institucion
2. Los privilegios de acceso a internet estaran limitados por los requerimientos de cada ususrios los cuales deberan estar directamente realcionados con sus funciones y responsabilidades laborales
3. los usuarios de la UIF que tenga acceso a internet no podran navegar o conectarse a sitios que no esten autorizados.
4. La Jefatura de Sistemas y Tecnologías de la Informacion de la UIF inpondran restriciones y utilizaa mecanismos de bloqueo de accesos a sitios no autorizados.
5. La Jefatura de Sistemas y Tecnologías de la Informacion de la UIF podra monitorear el uso de la conexión a internet por parte de los usuarios.
6. El uso inadecuado de la conexión a internet de la UIF sera reportado a la Direccion de la UIF.
7. Cualquier acceso a Internet no autorizado es enteramente responsabilidad del usuario solicitante.
8. Las Infraciones a la Politica de Seguridad de la Informacion de ASFI seran sancionadas de acuerdo al Reglamento Interno de Personal y normativa vigente.

Para llenado por Jefatura de Sistemas y Tecnologías de la Información

Proveído Jefatura de Sistemas	**Dirección Física de RED**	**Nombre de Equipo**

NIVEL DE ACCESO CATALOGADO Nivel 1 ☐ Nivel 2 ☐ Nivel 3 ☐ Nivel 4 ☐

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

ANEXO D - Formulario de Solicitud para Restauración de Password

	FORMULARIO DE SOLICITUD DE RESTAURACIÓN DE PASSWORD		**Fecha Solicitud**

Area Solicitante		
Nombre y Apellido del Solicitante	**Código**	**Sistema**

Justificación de la Restauración de Password	
Firma del Solicitante	Firma de Inmediato Superior Autorizando la Restauración solo en caso de no ser propietario de la Cuenta y password de Acceso.
Observaciones:	

Notas: **a) El presente Formulario deberá llevar las firmas correspondientes de lo contrario la Jefatura de Sistemas procederá con el rechazo de la presente solicitud.**

b) En caso de NO ser propietario de l Password y de ser necesario el Solicitante puede adjuntar el presente Formulario, documentación de respaldo para justificar la Solicitud la misma que deberá ser revisada por el Autorizador.

Unidad de Investigaciones Tecnológicas Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Tecnológicas Vo.Bo. J.V.C.G. JSTI

ANEXO E - FORMULARIO DE HABILITACION DE USUARIO

	FORMULARIO DE HABILITACION DE DE USUARIO	JSTI-US-V1	Fecha:

Solicitado por:	Código:
Cargo:	
Autorizado por:	Código:
Jefatura/ Dirección:	

N°	DESCRIPCIÓN DE USUARIOS OTORGADOS	SOLICITADO	OTORGADO
1	USUARIO DE DOMINIO		
2	CORREO ELECTRONICO		
S	USUARIO SADI		
4	USUARIO SISO		
5	USUARIO SISTEMA DE REGISTRO DE S.O.		
6	USUARIO SERVIDOR DE COMPARTIDOS		
7	USUARIO SB10		
8	USUARIO SISTEMA DE VIATICOS Y PASAJES (GOLONDRINA)		
9	PORTAL DE RECURSOS HUMANOS		
10	USUARIO SPO		

OTROS SERVICIOS	

Solicitado por:	Autorizado por:	Encargado JSTI	Conformidad

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

ANEXO F - GLOSARIO DE TÉRMINOS

Ambientes de Computo: Todo lugar donde se encuentren los equipos de computación centrales de la UIF (servidores, equipo de computación y otros).

Archivo Base: Archivo propio de la herramienta o manejador de correo electrónico que almacena los mensajes de correo electrónico recibidos, enviados, borrados, borradores, archivos adjuntos y otros, según las facilidades de la herramienta utilizada. Por ejemplo Microsoft Outlook los denomina Archivos PST.

Acceso Genérico: Es el conjunto de accesos y servicios que tienen en general todos los cargos. (ej. Todas las unidades y Direcciones que cuentan con acceso a Internet).

Acuerdo de Nivel de Servicio: (Service Level Agreement) Es un compromiso, normalmente por escrito, pactado entre un proveedor de servicio y un cliente o usuario. La función de este acuerdo es:

- Especificar los servicios a ser proporcionados por el proveedor.
- Especificar la calidad, seguridad, tiempo de entrega y características adicionales de los servicios pactados.
- Definir los recursos y disponibilidades que el usuario cliente y/o el negocio deben proveer como condicionante para cumplir con el acuerdo.

Administración de Redes: Definido como la suma total de todas las políticas, procedimiento que intervienen en la planificación. Configuración, control y monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos.

Autorización formal: Se refiere al tipo de autorización que deja un rastro o tiene características de trazabilidad, puede ser realizada mediante un formulario, circular interna, memo, correo electrónico u otro medio que cumpla la característica.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Baja: Es la marca a un usuario como "Baja", mismo que quedara inhabilitado de su ingreso al sistema computacional definitivamente.

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

Bloqueo: Es la baja por un periodo determinado de un usuario, pudiendo ser por vacaciones, baja médica u otra excusa.

Centro de Procesamiento de Datos (CDP) o Data Center: Es el ambiente donde se encuentran los equipos de sistemas centrales como ser Servidores, equipos de computación, equipos de telecomunicaciones, Central Telefónica, UPS's y otros.

Cuenta de usuario técnico: Se refiere a las cuentas de administración existentes en dispositivos o aplicaciones informáticas, por ejemplo root, oracle, Administrador, ADM, DBA, y otras cuentas necesarias para la administración de servicios informáticos.

Clave de Acceso: La clave de acceso (password) es el texto formado por varios caracteres de conocimiento único del usuario, que cumpla la función de autentificar su identidad ante los recursos informáticos.

Clave Trivial: Es el conjunto de caracteres que forman la clave de acceso inicial que avisa al usuario del sistema computacional, para que este acceda al mismo por primera vez, clave que deberá ser modificada inmediatamente.

Contingencias: Hechos fortuitos e imprevistos que alteran el normal funcionamiento de un dispositivo o proceso.

Custodio: Funcionario responsable del cuidado y preservación de un recurso tecnológico asignado a su persona para el cumplimiento de sus funciones.

Cuenta Genérica: Corresponde a aquella cuenta de correo electrónico que se refiere aun producto o servicio asignado a un cargo responsable institucional, por ejemplo domain@uif.gob.bo

Cuenta Personal: Corresponde a aquella cuenta de correo electrónico asignada a un funcionario especifico, por ejemplo juancito.pinto@uif.gob.bo

Dispositivos de red: Los dispositivos de red comprenden tarjetas de red, routers, switches, hubs y otros.

Escalar: Direccionar una actividad hacia un nivel superior desde un nivel inferior.

Elementos físicos: Los elementos físicos son conectores, cables, multiplexores, tarjetas.

Elementos de software: Los elementos de software son versiones de sistema operativo, parches y aplicaciones.

Facilidades: Todo el conjunto de dispositivos, instalaciones e infraestructura disponible para el desarrollo de operaciones en el Ambiente de Producción, involucra el área ISP (Infraestructura Services Provider). Por ejemplo, se considera parte de facilidades la instalación eléctrica, el aire acondicionado y otros.

Fichas técnicas: Conjunto de datos relacionados con cada dispositivo que reflejen sus características técnicas y permitan hacer un seguimiento durante su ciclo de explotación.

IDS: Sistema de Detección de Intrusos, es una herramienta de seguridad encargada de monitorear los eventos que ocurren en un sistema informático en busca de intentos de intrusión. Se incluyen en esta definición variaciones tales como HIDS y otros.

Incidente: Cualquier hecho o actividad aislada que suceda en el Ambiente de Producción o en el Ambiente de Desarrollo durante la fase de pruebas y afecte a la continuidad de procesamiento y la alta disponibilidad del negocio de la UIF. Estos o pueden afectar procesos

diarios, mensuales; detener, iniciar, reiniciar, bloquear o desbloquear tanto Servidores como programas y aplicaciones, así como el equipamiento en Producción (routers, switches, módems, firewalls y otros), ambientes de Información y Tecnología, facilidades y otros.

Incidente o violación de Seguridad: Esta definido como toda acción ejecutada o intento de acción sobre los recursos, que tenga la potencialidad o que ponga en riesgo su integridad, disponibilidad, eficacia, eficiencia, confidencialidad y/o fiabilidad en el procesamiento de información. Así mismo se considera un incidente de seguridad el abuso o mal uso de los recursos que perjudiquen a la UIF y/o estén en contra de su Normativa Interna.

Algunos ejemplos (lista no exhaustiva) de los eventos específicos considerados dentro de la definición de un "incidente de seguridad":

- Alteración no autorizada de la configuración de hardware definida según Normativa Interna.
- Instalación no autorizada de software.
- Cambio o sustracción no autorizada de partes.
- Movimiento no autorizado, cambio de su ubicación física dentro y/o fuera de los ambientes de la UIF.
- Uso para fines propios y/o ajenos a los de la UIF.
- Explotación no apropiada que provoque el daño físico del dispositivo.

Información confidencial: Todo dato o documento que ha sido generado en la Institución.

Instancia Afectada: Unidad o Dirección que fue afectada por un problema o incidente dentro de la UIF, como por ejemplo DDO, cualquiera de las Direcciones, Jefaturas, Propietarios de la información, Asesor legal, y otros.

Intento de Intrusión: Cualquier intento de comprometer la confidencialidad, integridad, o disponibilidad de cualquier sistema informático, o de eludir los mecanismos de seguridad de este.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Manejo de Incidentes: Actividades, realizadas para restaurar las operaciones normales de servicio de la manera mas rápida, minimizando el impacto negativo en las operaciones del negocio. Este manejo esta enfocado a:

Unidad de Investigaciones Financieras Vo.Bo. J.I.C.G. JSTI

- Restauración de los servicios.
- Detección del incidente o problema y su registro.
- Clasificación y soporte inicial.
- Investigación y diagnostico del incidente del problema.
- Solución.
- Verificación de la recuperación del proceso o restauración del servicio afectado.
- El Cierre del incidente.

Manejo de Problemas: Actividades realizadas para minimizar el impacto negativo de problemas en el negocio, los cuales pueden ser causados dentro la infraestructura de

Información y Tecnología y otras, como también para prevenir la recurrencia de problemas relacionados a estos errores. Manejo de Problemas se enfoca en la raíz de los problemas, identifica soluciones alternativas o definitivas y elimina de manera permanente estos errores. Las actividades típicas de manejo de problemas incluyen:

- Control del problema.
- Control de error.
- Prevención proactiva del problema.
- Revisión de los problemas más recurrentes.

Material Sensible: Es todo material que contiene información, tales como cintas, CDs, diskettes y otros. También es material sensible el equipamiento técnico tales como partes, conectores, llaves y otros.

Medios removibles y/o móviles: Medio de almacenamiento como disco compacto, disco rígido, diskettes, memoria de circuito y dispositivos inalámbricos, que pueden ser removido y trasportados fácilmente por el usuario final.

Medios de Almacenamiento Masivo: Se constituyen aquellos elementos o dispositivos en los que se puede almacenar información , por ejemplo: Flash Memorys, Discos duros externos, smartfones con capacidad de almacenamiento y otros similares.

Mensajes tipo Cadena (spam): Mensaje de correo electrónico por lo general anónimo, en el que se solicita al destinatario reenviar al mismo a varias personas recurriendo a distintos argumentos para convencerlo.

Multimedia: Conjunto de dispositivos electrónicos con capacidad de reproducción y procesamiento de voz, imagen y datos, por ejemplo: parlantes y proyector.

Perfil: Conjunto de acciones y eventos agrupados que se ejecutan en el sistema computacional.

Problema: Cualquier hecho o actividad que suceda, de manera recurrente, en el Ambiente de Producción y afecte la continuidad de procesamiento y la disponibilidad del negocio de la UIF. Estos pueden afectar procesos diarios, mensuales; detener, iniciar, reiniciar, bloquear o desbloquear tanto Servidores como programas y aplicaciones, así como el equipamiento en Producción (routers, switches, modems, firewalls y otros), ambientes de Información y Tecnología, facilidades y otros.

Propietario o Dueño de la Información: Responsable por los datos e información contenida en las bases de datos, por los accesos usuarios y por las actividades que puedan comprometer la información bajo su custodia. Normalmente la vinculación esta en función de su cargo y responsabilidad.

User – ID: Identificación única del usuario ante un determinado sistema.

Usuario: Denominado también Usuario final. Todo empleado de la UIF que tiene interacción con los sistemas informáticos de la UIF, por medio de la infraestructura tecnológica.

Recursos Informáticos: Se hará mención de igual manera a Recursos de Tecnología, Recursos Informático, Agrupación de los objetos, inmuebles y personas relacionadas con el procesamiento de la información y la JSTI. Comprende cinco grandes grupos: Datos, aplicaciones, tecnología, infraestructura y gente.

Recursos de Red: Servicio destinado a apoyar el trabajo del personal interno de la Institución. Ejemplo de estos servicios son la red interna, Internet, correo electrónico, servidores y otros.

Responsable: Función asignada a personal de Información y Tecnología relacionada con actividades técnico operativas de la Administración de Problemas e Incidentes descritas en esta norma. Las responsabilidad no sugiere necesariamente un cargo, sino mas bien una función que puede ser asignada a cualquier cargo en la JSTI.

Requerimiento del Usuario: Solicitud ingresada por el usuario final en el servicio de Mesa de Ayuda. Tiene un número único que lo identifica.

Seguridad Física: Condiciones que permiten estabilidad del ambiente informático respecto a los riesgos de interrupción física de la continuidad de procesamiento, tales como incendios, daños intencionados y otros.

Seguridad Lógica: Condiciones del software que permiten estabilidad en el ambiente informático respecto a los riesgos de interrupción del software. Tales como cambio en programas, accesos no autorizados, eliminación de información y otros.

Sistemas Informáticos: Cualquier aplicación interna o externa que es requerida para el giro del negocio de la UIF.

Soporte Técnico: Ayuda de tipo técnico para usuarios finales de la UIF. Estas tareas incluyen entre otras, la administración de los equipos, la instalación de aplicaciones, el mejoramiento de hardware, la atención de problemas y la actualización de software en general.

TelKey: es la bóveda exclusiva para sistemas donde se almacena claves y llaves, tanto físicas como lógicas. Su ubicación dependerá de la:

- Independencia de Administración (segregación de funciones).
- Disponibilidad de Acceso.
- Seguridad Física del ambiente.

Unidad de Investigaciones Financieras Vo.Bo. C.L.B. JSTI

Unidad de Investigaciones Financieras Vo.Bo. J.L.C.G. JSTI

Virus: Se considera como virus informático a todo aquel programa que altere, dañe o modifique configuración, programas y/o contenidos de cualquier equipo de la red sin autorización y conocimiento pleno del usuario. En la presente norma no se hacen distinciones entre las formas y tipos de estos programas, que comprenden los troyanos, gusanos, adware, spyware y toda variante actual o futura.

Zonas de Información y Tecnología: Son los diferentes ambientes donde la JSTI tiene recursos tecnológicos utilizados para el procesamiento de la información de la UIF, estos

pueden contener Servidores de archivos, aplicaciones, dispositivos de comunicaciones, generadores de energía auxiliar y otros, tanto en la oficina principal como en las departamentales.