MANUAL

DE

DISPOCISIONES

DE TECNOLOGÍA DE

INFORMACIÓN

Y SEGURIDAD DE TI

INDICE

DESCRIPCIÓN DE LAS MODIFICACIONES:	Periodo de mantenimiento del Ups y de aire acondicionado Se agrega en el capítulo IX Otras consideraciones: *En caso de implementación de Nuevas Tecnologías (Software y hardware), los responsables de las áreas deberán comunicar vía correo electrónico al Departamento de Seguridad TI, a fin de analizar los riesgos asociados y emitir un parecer técnico para su consideración.*
FECHA DE VIGENCIA:	**15.03.2024**

Proyectado por:	Diana Orzuza **Jefe de O y C**
	Carlos Paniagua **Sub-Gerente de Desarrollo**
	Diego Bittar **Sub-Gerente de Redes, Infraestructura y Base de Datos**
	Humberto Ortega **Sub-Gerente de Seguridad de TI**
Revisado por:	Alfredo Zuccotti **Gerente de TI**
	Diego Segovia **Gerente General**
Aprobado por:	Acta N° 49/2024 del 12/03/2024

A. INTRODUCCIÓN

Se ha desarrollado el presente documento para establecer los criterios y las responsabilidades del área de Tecnología de Información.

Con este manual, se pretende trazar los lineamientos bajo la responsabilidad del área de Tecnología de la Información, como de los usuarios del uso de la misma, a fin de que toda la institución este en contexto, se realice de una manera clara, precisa, transparente y lo más real posible, donde se respeten los principios éticos que dentro del marco normativo, produciendo así una escala de valores de hechos y formas de comunicación dentro de la institución.

El Manual contiene capítulos, donde cada uno de ellos está compuesto por su objetivo y sus disposiciones generales.

CAPITULO I. ACCIONES PARA LLEVAR A CABO EN CASO DE ATAQUES O ESCANEADO DESDE LE RED EXTERNA

1. Objetivo:

Con las Acciones se pretende evaluar y minimizar el impacto de posibles ataques o escaneados desde la red externa, ante las siguientes situaciones:

- Primeras medidas a adoptar ante un posible ataque.
- Evaluación de los daños.
- Acciones correctivas y legales.
- Procedimientos para restaurar los daños.
- Aspectos importantes a considerar.

2. Disposiciones generales:

Primeras medidas:

a) Revisar si es un ataque real o es una falsa alerta del IDS.

b) Si es un escaneo o ataque real, evaluar la posibilidad de bajar el servicio disponible en Internet que está siendo objeto de ataque.

c) Escalar la comunicación a los responsables del servicio y de la tecnología afectada.

Evaluación de daños:

a) Verificar:

i) El nivel de penetración llevada a cabo;

ii) Si se alteraron o borraron datos en la base de datos;

iii) Si se crearon puertas traseras;

iv) Si se crearon usuarios nuevos a nivel de base de datos o servidores;

v) Si se eliminaron archivos, etc.

b) Documentar todo lo ocurrido y las acciones llevadas a cabo.

c) Resguardar toda la documentación, logs y toda evidencia válida.

Acciones correctivas y legales:

a) Revisar si es una dirección IP de Paraguay o una foránea.

b) Si es una dirección IP de Paraguay, ver cuál es su proveedor de Internet, en caso de que no hayan ocurrido todavía daños, comunicar al proveedor la situación a fin de que advierta al usuario que de continuar con el intento la Universitaria iniciará acciones civiles y penales contra quienes corresponda, por daños y perjuicios.

c) Derivar la evidencia necesaria al área Jurídica para entablar acciones civiles y/o penales que correspondan, contra el dueño de la dirección IP por violación o intento de violación de lo que establece el Código Penal.

d) Si es una dirección IP del extranjero, ver la forma de bloquear o ignorar en los routers el tráfico proveniente de esa dirección IP específica, o en casos extremos bloquear esa red a fin de evitar nuevos ataques en caso de que tenga una dirección IP dinámica (que se cambie cada vez que se conecta a su ISP).

Restaurar Daños:

a) Restaurar los archivos dañados con backup o reinstalar software.

b) Eliminar usuarios creados, puertas traseras abiertas, cerrar puertos abiertos, etc.

c) Corregir datos modificados si los hubiera.

Importante:

a) Nunca hacer ping a la dirección IP del Hacker porque puede delatar su presencia y puede emprender ataques más severos al servidor provocando un DoS.

b) Nunca devolver el ataque, porque puede que este se esté realizando desde un equipo que fue tomado por un Backdoor, y un ataque a ese equipo nos puede

acarrear una demanda. Tampoco es conveniente devolver el ataque porque se desconoce la fuerza del atacante y las debilidades descubiertas en nuestro sistema.

c) Tener siempre copias de respaldo a fin de minimizar los daños provocados y disminuir el tiempo de reposición del servicio.

Alertas y Revisión de Seguridad:

a) **IDS**: Se tienen instalados equipos con Sistemas de Detección de Intrusos (IDS) que realizan una verificación constantemente en sus logs, y avisarán por e-mail a los encargados de la Administración de Seguridad de TI en caso de que ocurra cualquiera de los siguientes ataques:

"Alerta Portscan"	Escaneo de Puertos
"Alerta NMAP"	Utilización de la Herramienta NMAP contra algún equipo de la red
"Alerta SSHD"	Intento de logueo en algún servidor
"Alerta passwd"	Intento de cambio de contraseña
"Alerta overflow"	Intento de provocar un desbordamiento de memoria
"Alerta SNMP trap"	Intento de provocar trampa en el protocolo de tráfico de red SNMP
"Alerta DOS"	Intento de provocar ataque de Denegación de Servicio
"Alerta SCAN"	Detecta escaneados FIN (solo puertos TCP abiertos) y escaneados SYN (Es conocido como escaneo half-open, el motivo es por que no se completan los 3 pasos de la conexión, primero se envía el paquete SYN, luego si la respuesta es SYN/ACK esto indica que el puerto esta en modo

	de escucha y si la respuesta es RST/ACK indicaría que el puerto no esta a la escucha).
"Alerta BAD-TRAFFIC"	Tráfico proveniente desde el puerto 127.0.0.1 para que se engañe a sí mismo
"Alerta AgentX"	AgentX de SNMP que permite manejar múltiples subagentes
"Alerta Atck"	Ataques de cualquier tipo
"Alerta Retriever"	ICMP L3retriever ping (ojo porque hay muchos falsos positivos)

b) **AIDE**: También se cuenta con un programa de verificación de integridad, llamado AIDE, con el cual se realiza la verificación de integridad de los archivos. Para verificar la integridad se genera un archivo de verificación sobre redundancia cíclica inicial, y luego cada cierto tiempo para ver si alguno de los archivos mencionados en su aide.conf fueron alterados. El comando para generar el check es el siguiente: aide -c /etc/aide.conf –check

CAPITULO II. ENLACES REDUNDANTES PARA CONEXIÓN DE LAS SUCURSALES

1. Objetivo

Definir las acciones a seguir para mantener conexión de dos enlaces en forma redundante para las Sucursales de Universitaria.

2. Disposiciones generales:

a) La Sucursal debe contar con un Ruteador con capacidad de administrar dos enlaces de comunicación.

b) El Ruteador de la Sucursal debe tener conectado dos enlaces de comunicación de distintos proveedores.

c) Se deben tener configuradas dos VPN's con Casa Matriz, una considerada como principal y otra como secundaria, tomando en cuenta la que ofrezca mayor velocidad y/o ancho de banda.

d) En caso de caída de la VPN principal, el Ruteador debe cambiar al enlace secundario utilizando algún protocolo de ruteo que debe estar configurado previamente en el equipo.

e) Cuando el enlace principal vuelva a estar arriba el Ruteador debe volver a cambiar automáticamente para volver al trabajo normal.

f) Los Operadores de Redes realizarán pruebas periódicas del funcionamiento correcto de la redundancia de enlaces con las Sucursales, e informar al respecto al superior inmediato, a fin de tomar las acciones que sean necesarias.

CAPITULO III. ACCESO DATA CENTER

1. Objetivo:

Documentar la operativa y medidas de seguridad para el ingreso y egreso físico de personas al Datacenter.

2. Definiciones:

Datacenter: Centro de Cómputos, Sala de Servidores.

Personal Autorizado: Se refiere al personal del Área de Tecnología en condiciones de ser autorizado a ingresar al Datacenter (**Subgerente de infraestructura**, Jefe de base de datos, **Subgerente** de Seguridad de TI, Operadores de Seguridad de TI, Operadores de Redes, Operadores de Base de Datos, Gerente de TI, Sub Gerente de **Desarrollo**).

Personal Ajeno: Se refiere al personal de las empresas que trabajan como proveedores externos de servicios e insumos y necesitan acceso a ciertas áreas del Datacenter para casos de mantenimiento, implementación y/o mitigación de incidentes. Al mismo tiempo se toma como personal ajeno a aquellas personas designadas para visitar nuestras instalaciones con fines de exponer la infraestructura que poseemos y podría servir como ejemplo para otras empresas.

Dependencias: El Datacenter está sectorizado con el fin de mantener la integridad y confidencialidad de los equipos que se alojan en el mismo.

Las dependencias son:

- Computer Room - Sala de Servidores
- Entry Room 1 / Sala de Proveedores 1
- Entry Roon 2 / Sala de Proveedores 2
- Deposito
- NOC / Oficinas de monitoreo de infraestructura y networking
- MDA 1 / Sala de Networking 1

- MDA 2 / Sala de Networking 2
- UPS 1 / Sala de UPS 1
- UPS 2 / Sala de UPS 2
- Salta Técnica

Zonas: Las zonas son aquellos sitios que comprenden más de una dependencia.

ZONA 1: MDA1/UPS1

ZONA 2: MDA2/UPS2/Sala Tecnica/Entry Room2

3. Acceso

Personal Autorizado

- ***Subgerente de Redes e infraestructura***
- *Operador de Redes*
- *Operador de Redes*
- *Jefe de Base de Datos*
- *Operador de Base de Datos*
- *Operador de Base de Datos*
- *Gerente de TI*
- ***Subgerente de Desarrollo***
- *Jefe de Seguridad de TI*
- *Operador de Seguridad de TI*

El personal autorizado tendrá acceso al Datacenter en cualquier momento del día, a cualquiera de las dependencias, ya sea para instalaciones, verificaciones, procedimientos y/o acompañamiento de personal ajeno a la institución.

Personal Ajeno

El personal ajeno debe ingresar al Datacenter acompañado de al menos 1(un) personal autorizado. Deberá completar el Libro de Actas de Ingreso de Personal Ajeno al Datacenter**.** El

mismo debe encontrarse en la puerta de ingreso a la oficina de TI, la cual conduce al Datacenter.

Los datos que completa son:

- ✓ Fecha
- ✓ Horario de Entrada
- ✓ Horario de Salida
- ✓ Nombre y Apellido de la persona que ingresa
- ✓ Tarea a realizar
- ✓ Sector / Empresa

Al finalizar su visita, el personal ajeno deberá firmar el libro de actas y colocar la hora de salida, el mismo será supervisado por la secretaría del área de TI.

4. Otras consideraciones:

- El personal ajeno NO tendrá acceso a todas las dependencias. Los mismos serán establecidos según el tipo de trabajo a realizarse dentro del mismo, establecido de la siguiente manera:
  1. Los ISP o proveedores de enlaces solo podrán tener acceso a las dependencias de Entry Room 1 y Entry Room 2
  2. Las empresas encargadas de implementaciones y mantenimientos a nivel de servidores o infraestructura solo tendrán acceso al Computer Room, al MDA 1 y MDA 2
  3. Las empresas encargadas del área de Networking solo podrán tener acceso al MDA1 y MDA 2
  4. Las empresas encargadas de la parte de Seguridad de TI solo podrán tener acceso al Computer Room, MDA 1 y MDA 2.
  5. Las empresas encargadas del mantenimiento de las UPS solo tendrán acceso a la sala de UPS1 y UPS2

6. Las empresas encargadas del mantenimiento de los aires tendrán acceso a todas las dependencias.

Esto debe verificarse con el personal autorizado designado en el momento del ingreso

- Para el acceso al computer room se deberá pisar indefectiblemente las alfombras Sticky Mat de 30 hojas cambiales ubicadas en la entrada al Computer Room, en la Zona 1, en Zona 2 y en el Entry Room 1. Las mismas sirven para aislar de residuos el calzado de los visitantes.
- El libro de actas quedará a cargo de la secretaría de TI, y el mismo puede ser solicitados en cualquier momento por algún superior.
- No se podrá ingresar con gorras, celulares ni comida.

CAPITULO IV. ADMINISTRACIÓN DE MODULOS DEL SISTEMA

1. Objetivo:

Establecer las normas a ser consideradas para la correcta administración de los módulos de los sistemas utilizados en la Universitaria.

2. Generalidades:

a) Se designará un encargado de cada módulo componente de los sistemas utilizados en la Cooperativa, de manera a lograr un eficiente manejo de los mismos. Esta designación será realizada por el Gerente del área respectiva.

b) La clasificación de la información (tablas y programas) en base al grado de criticidad, será responsabilidad de los Gerentes responsables de Módulos.

c) Las solicitudes de desarrollo de nuevos programas y las de modificación de programas existentes, deberán contar con el visto bueno del Encargado del módulo en cuestión, y del Gerente del sector.

d) Las Gerencias responsables de cada sistema o módulo tendrán la responsabilidad de definir los roles de acuerdo a los perfiles de los usuarios involucrados en su utilización, teniendo en cuenta que el acceso y uso de la información, sea efectuado según las funciones establecidas y las tareas desarrolladas, teniendo siempre en cuenta aspectos de control interno.

e) Por otro lado, el Administrador de Seguridad de TI, será responsable de verificar que los accesos y usos solicitados correspondan al perfil del usuario, cuenten con la aprobación de la Gerencia Responsable del Módulo y se mantengan actualizados.

f) En la siguiente tabla se especifican las Gerencias responsables de los distintos módulos y sistemas utilizados en la Cooperativa:

MÓDULOS		
DESCRIPCIÓN	**FINALIDAD**	**AREA RESPONSABLE**
Ahorros	En este módulo se realizan todas las operaciones correspondientes a Apertura y Cancelación de Cuentas de Ahorro a la Vista, Ahorro Programado y Plazo Fijo, Débitos Automáticos, Tarjetas de Débito, y su interacción con los demás módulos.	Gerencia de Ahorros
Aporte	En este módulo se realizan todas las operaciones correspondientes a Aporte, así también el mantenimiento de las cuotas de aportes para los socios a cada año.	Gerencia de Servicios
Socios	En este módulo se realiza la carga de solicitudes de ingreso de socios, mantenimiento de sus datos, consultas, etc.	Gerencia de Servicios cooperativos
Solidaridad	En este módulo se realizan las transacciones correspondientes a subsidios y premios por solidaridad. Se realiza el mantenimiento de las cuotas de solidaridad para los socios a cada año.	Gerencia de Servicios cooperativos
Créditos	A través de este módulo se realizan todas las transacciones correspondientes a un crédito; recepción y carga de solicitud, análisis del crédito, desembolso, emisión de cheque y seguimiento.	Gerencia de Productos Crediticios
Mypes	Este módulo es utilizado por los Oficiales de Microfinanzas, para gestionar los créditos empresariales.	Gerencia de Productos Crediticios
Tarjetas	En este módulo se realiza la carga de solicitudes,	Gerencia de Productos Crediticios

	análisis, y aprobación de las tarjetas de crédito emitidas por la Cooperativa.	
Tarjetas Valores	En este módulo se realizan los procesos automáticos de cargas de tarjetas, asignación de movimientos, detalles y resumen de los plásticos.	Gerencia de Productos Crediticios
Auditoría Interna	Este módulo es utilizado por Auditoría Interna para el desarrollo de sus funciones respectivas. Cuenta con opciones de consulta de las distintas áreas (ahorros, créditos, tesorería y cajas, etc.)	Gerente de Auditoría Interna
Caja Chica	En este módulo se registran todos los gastos que están destinados a cubrir facturas, recibos o adelantos para gastos menores.	Gerencia Financiera
Conciliación	Este módulo tiene el objetivo de agrupar en un lugar específico, todos aquellos procesos, informes o listados, necesarios para efectuar conciliaciones de los Módulos de Ahorros y Créditos.	Gerencia Administrativa
Contabilidad	Módulo donde se realizan los asientos, conciliaciones, nuevas cuentas contables, y la emisión de los documentos que son requeridos por los distintos Departamentos de la Universitaria, y las entidades externas.	Gerencia Administrativa
Presupuesto	A través de este módulo se asigna el importe al cual se desea llegar a cada año y el control de los mismos por medio de reportes.	Gerencia Financiera
Registro de Firmas	Este módulo es utilizado para registrar y verificar las firmas de los socios de la Cooperativa.	Gerencia de Ahorros
Cierre		Gerencia de TI

	En este módulo se corren los procesos que corresponden al cierre informático de la Universitaria de cada día, donde se calculan los saldos diarios de cuentas de ahorro que se utiliza para la capitalización a fin de mes.	
Asuntos Legales	En este módulo se pueden realizar consultas y modificaciones de las transacciones de los socios que se encuentran en estado judicial.	Asuntos Legales
Tesorería	En este módulo se realizan todas las operaciones correspondientes al área de cajas (Apertura y cierre de caja, Arqueo, transacciones, operaciones varias).	Gerencia Financiera
Call Center	En este módulo pueden realizarse consultas de modo a facilitar datos al socio vía telefónica, como así también recibir denuncias por robos o extravíos de tarjetas.	Gerencia Comercial
Riesgos	Sistema de programas utilizado para la administración y control de riesgos en los servicios financieros de la Cooperativa	Sub Gerencia de Riesgos
Educación	Módulo a través del cual se gestionan y administran actividades del Comité de Educación, eventos, cursos, etc.	Sub Gerencia de Educación
Finanzas	Módulo que permite administrar y controlar las operaciones financieras de la institución, libro bancos. Informes al INCOOP, y reportes financieros.	Gerencia Financiera
Prevención de lavado de dinero	Módulo por el cual se gestiona el control de operaciones de socios. Generación de perfil de riesgos y seguimiento de transacciones para informes a la SEPRELAD.	Gerencia de Cumplimiento

OTROS SISTEMAS		
DESCRIPCIÓN	**FINALIDAD**	**AREA RESPONSABLE**
Envío de Mensajes	Este sistema permite el envió de mensajes a los socios sobre los servicios y actividades de la Cooperativa.	Gerencia Comercial
Sistema de Adquisiciones e Inventario	En este módulo se realizan los pedidos de papelería y útiles, servicios de mantenimientos de bienes, adquisición de nuevos bienes, depreciaciones y revalúo del activo fijo.	Gerencia Administrativa
Sistemas de Pedidos	Este sistema permite realizar pedidos al área de Tecnologías de Información (TI), relacionados a ajustes o modificaciones al sistema informático.	Gerencia de T.I.
Presupuestos COLAC	Es un sistema utilizado para la planificación presupuestaria de las distintas sucursales de la Cooperativa.	Gerencia Financiera
Sistema de Recursos Humanos	Este sistema es utilizado por el Dpto. de Recursos Humanos, para el control de asistencia, permisos, vacaciones, pago de salarios, y otros, de los empleados de la Cooperativa.	Gerencia Administrativa
WEB		
DESCRIPCIÓN	**FINALIDAD**	**AREA RESPONSABLE**
Web	Este sistema permite al socio realizar múltiples transacciones a través de internet, las 24 horas del día.	Gerencia de Ahorros
Prevención de Lavado de dinero	Este sistema es utilizado, para el registro de datos	Gerencia de Cumplimiento

	de socios y elaboración de perfiles, como así también para el monitoreo de transacciones.	
Data Scan	Este sistema se utiliza para la digitalización de los documentos proveídos por los socios para sus transacciones dentro de la Cooperativa.	Digitalización
CU Clasificados	Este sistema permite a los socios vender y/o comprar productos o bienes ofertados a través de internet.	Gerencia de Ahorros
App Universitaria 24hs	Sistema que permite al socio realizar operaciones desde dispositivos celulares, a través de la APP Universitaria.	Gerencia de Ahorros

V. CALIDAD DE SOFTWARE

1. Objetivo:

La calidad del software comprende distintos aspectos como estética (que sea agradable a la vista), funcionalidad (que sea fácil de usar), eficiencia (que se ejecuten con rapidez y precisión los procesos), etc. Lo que distingue al software de otros productos industriales es que no es de naturaleza material, no se puede tocar. Por tanto, no resulta viable hacer una valoración del mismo en base a una impresión rápida o análisis del aspecto ni en base al coste de materiales componentes, sin embargo, en informática, el término métrica hace referencia a la medición del software en base a parámetros predeterminados, como puede ser el número de líneas de código de que consta o el volumen de documentación asociada.

.A partir de este concepto de calidad del software, podremos llegar a deducir cuatro objetivos:

a- Calidad de los Requerimientos: el objetivo de esta meta es que los documentos requeridos estén completos, no sean ambiguos y sean entendibles. Esta meta tiene los siguientes atributos: (1) Ambigüedad: requerimientos con múltiples significados, (2) Integridad: puntos a ser especificados, (3) Facilidad de entender: documento legible y (4) Trazabilidad: trazabilidad de los requerimientos generales respecto del código y de las pruebas.

b- Calidad del Producto: un objetivo importante de un proyecto de desarrollo de software es desarrollar código y documentación que se correspondan con los requerimientos del proyecto. Esta meta u objetivo tiene los siguientes atributos:

- Estructura / Arquitectura: la evaluación de un módulo para identificar posibles errores e indicar problemas potenciales en la facilidad de uso y facilidad de mantenimiento.

- Reutilización: utilizar el software en diferentes contextos o aplicaciones.

- Facilidad de mantenimiento: es el esfuerzo requerido para localizar y corregir un error en un programa.

- Documentación: tener la adecuada documentación del código interno y la documentación externa.

c- Efectividad de la implementación: el objetivo de la efectividad de la implementación es maximizar la efectividad de los recursos dentro de las actividades programadas en el proyecto. Los atributos de este objetivo son:

- Uso del recurso: el uso del recurso relacionado a la etapa apropiada del proyecto.

- Cumplimiento de los porcentajes: avances realizados en los distintos puntos.

d- Efectividad de la prueba: los objetivos de la prueba de efectividad es ubicar y reparar las fallas del software. El atributo es la corrección. Una vez generado el código, se realizan pruebas de unidades, pruebas finales y pruebas de aceptación.

2. PRUEBA DE PROGRAMAS Y SISTEMAS:

a) A fin de asegurar que el programa produzca los resultados definidos en las especificaciones funcionales, el Desarrollador a cargo utilizará los datos de prueba para asegurarse que el programa produce los resultados correctos;

o sea, que se produzca la acción correcta en el caso de datos correctos o el mensaje de error y una acción correcta en el caso de datos incorrectos.

Una vez terminada la programación, el Analista a cargo del sistema volverá a usar los datos de prueba para asegurarse que el programa o sistema produce los resultados correctos. En esta ocasión, el Desarrollador concentrará su atención también en la interacción correcta entre los diferentes programas y el funcionamiento con el sistema.

b) El funcionario del área de Calidad de Software, será responsable de mostrar en forma general los requisitos mínimos necesarios para que la implementación del sistema resulte exitosa, como así también de la propia implementación de Sistemas.
c) El Desarrollador que realizó el nuevo programa o la modificación de uno existente, deberá proveer suficiente información para que el encargado del área de Calidad de Software pueda realizar las pruebas pertinentes.
d) En el caso de Nuevos Programas, para la habilitación de permisos a usuarios del Sistema, el área de Calidad de Software remitirá para el efecto, al Dpto. de Seguridad de TI, un correo una planilla con los siguientes datos:
    - Nro. del Pedido al cual hace referencia el programa.
    - Permisos sobre los objetos de la Base de Datos que requerirá el programa.
    - Grupo de Usuarios que podrán acceder al programa (preferentemente clasificados por cargo).
    - Nombre que tendrá el programa dentro del Menú.
    - Ubicación del programa dentro del Menú.

3. MANTENIMIENTO Y/O CAMBIOS EN PROGRAMACION EXISTENTE

a) El usuario a cargo de la modificación deberá solicitar, mediante la Hoja de Pedido la modificación del dato, el cambio deseado ó la verificación del programa.

b) El Administrador de Proyecto viabilizará la modificación y asignará el pedido al Desarrollador.

c) El Desarrollador, analizará y definirá el programa siguiendo los elementos definidos para el diseño de Sistemas. Este Desarrollador debe cumplir con los elementos definidos para la Documentación de Programas y solicitará al área de Calidad le acompañe en la comprobación de que el trabajo realizado satisface la Hoja de Pedido; efectuará las pruebas requeridas y requerirá al usuario evidencia de aceptación final, dentro del Sistema de Pedidos. Además, deberá llenar dentro del Sistema de Pedidos las especificaciones de programas, disparadores, funciones, librerías, indicando con ello que deberá moverse del área de prueba a Producción.

d) El propietario del sistema es decir cada encargado de módulo deberá autorizar toda solicitud de cambios a programación existente en Sistemas que ya están en producción. Las oficinas de Tecnologías de Información son custodios de los datos y programas. Sin embargo, los encargados de Módulos dependiendo del caso son los únicos que pueden autorizar cambios a los mismos o la distribución de la información que estos producen.

e) Los funcionarios del área de Calidad de Software, deberán realizar pruebas dentro del proceso de control de calidad para identificar a las investigaciones empíricas y técnicas, cuyo objetivo es proporcionar información objetiva e independiente sobre el producto a ser utilizado o en producción.

Las pruebas son básicamente un conjunto de actividades dentro del desarrollo del Software. Dependiendo del tipo de pruebas, estas actividades podrán ser implementadas en cualquier momento de dicho proceso de desarrollo.

El contexto de pruebas será siempre el mismo pero los enfoques y demás elementos que los condicionen como ser técnicas, documentación, ejemplos, entre otros deben estar bien definidos.

Se identifican dos ambientes en los que se podrá desenvolver; pruebas que se realizan sin ejecutar el código de la aplicación, para ver el flujo de los datos y como se registraron dentro de la base de datos. Pruebas que requieren la ejecución de la aplicación a fin de identificar como se comporta el Software ante determinadas situaciones.

A fin de poder ordenar y hacer lo más eficiente posible este proceso se definen las siguientes pautas para ser utilizadas dentro del mismo:

- Comprender el problema antes de corregirlo.
- Comprender el programa, no solo el problema.
- Confirmar que se genera el error al ejecutar el programa.
- Identificar y corregir el problema.
- Volver a ejecutar el programa a fin de verificar que la modificación o corrección es la correcta y no afecta a otras situaciones.
  Para corregir los casos de error es necesario tener en cuenta estas sugerencias:

- Estabilizar el error; hallar un caso de prueba que produzca el error que sea lo más simple posible

- Localizar la fuente del error; observar el comportamiento bajo condiciones controladas
- Corregir el error; ver la lógica de la programación y la sintaxis
- Probar la corrección; con el caso del error y las otras situaciones posibles.
- Buscar errores similares; verificar si existe otras partes del programa donde pudiesen presentarse el mismo error.

  Las pruebas que no estaban incluidas en el plan, se puede llegar a identificar y por sobre todo por medio del proceso de pruebas corregir y evaluar la calidad de la herramienta con la cual se cuenta.

CAPITULO VI. LENTITUD DE COMUNICACIÓN CON LAS SUCURSALES

1. Objetivo:

Describir el procedimiento a seguir para analizar los motivos de lentitud en la comunicación con una o varias sucursales de manera a disminuir la cantidad de reclamos y el tiempo en que demora determinar y solucionar el inconveniente

2. Disposiciones generales:

a. Las máquinas de Operaciones de Redes deberán tener abierto algún software de monitoreo de tráfico de Red.

b. Ya sea que la sucursal realice un reclamo o en el Software de monitoreo se visualice el problema, el Área de Redes deberá analizar el caso y determinar cuál es el inconveniente.

c. Desde una consola del DOS se podrá hacer un “ping” con la opción “-t” apuntando al Ruteador de la Sucursal a fin de monitorear mejor el comportamiento de la comunicación.

d. El Operador de Red deberá revisar cuál es el caso, si es una saturación de ancho de banda se debe monitorear cuál es la causa y dar aviso a la Sucursal en caso de que sea una PC que está traficando gran cantidad de información. El Sub Gerente o el funcionario a cargo de la Sucursal deberá decidir si el proceso que está saturando el ancho de banda será cancelado o no.

e. En caso de ser un inconveniente con el proveedor se debe hacer el reclamo correspondiente a la empresa responsable. De acuerdo a la respuesta del Carrier de comunicación se tomarán las medidas correspondientes.

f. Si la empresa comunica que el inconveniente va a tomar un tiempo en solucionarse, el Operador junto con su superior inmediato, determinará si sería más conveniente conectar directamente al enlace de backup, para lo cual será necesario bajar

manualmente el túnel de conexión del proveedor principal para que así el enlace de backup se levante de manera automática.

g. El Operador de Red realizará el seguimiento correspondiente e informará a los superiores y a la Sucursal afectada, por medio de un email, una descripción del problema, el procedimiento que se realizó y el tiempo en que se estaría solucionando definitivamente en caso de que dure un periodo prolongado.

CAPITULO VII. MANTENIMIENTO DE EQUIPOS DE LA SALA DE SERVIDORES DE MATRIZ Y SUCURSALES

1. Objetivo:

Establecer las normas a seguir para la realización de los mantenimientos preventivos de equipos ubicados en sala de servidores de la Casa Matriz y Sucursales de la Universitaria.

2. Disposiciones generales:

Servidores:

- Período de Mantenimiento: Realizar el mantenimiento preventivo de los servidores una vez al año tanto para Casa Matriz como Sucursales de Universitaria

- Días y Horarios: Estos servicios serán realizados en días y horarios en que los servicios ofrecidos a los socios no se vean afectados o mínimamente afectados.

- Áreas a informar: Se dará conocimiento a la Gerencia de TI. Se informará a la Gerencia General y Consejo de Administración solo en caso de que se vean afectados servicios utilizados por los socios de la Universitaria. En caso de equipos de Sucursales se deberá coordinar con el Subgerente de la sucursal afectada.

- Periodos de permanencia fuera de servicio: En caso que algún servicio que afecte a los Socios quedara sin funcionar, por el mantenimiento se informará previamente a la Gerencia General y/o Consejo de Administración el periodo en que los servicios estarían abajo.

UPS's de Sala de Servidores (Matriz):

- Período de Mantenimiento: El mantenimiento preventivo de UPS's de Sala de Servidores de Casa Matriz se deberá realizar cada **6 (seis)** meses por técnicos externos a la cooperativa en coordinación con el área de Redes y/o Base de Datos de TI. Las UPS's

de la Sala de máquinas deberán tener un cambio preventivo de baterías cada dos años aproximadamente.

- Días y Horarios: Estos servicios serán realizados en días y horarios en que los servicios ofrecidos a los socios no se vean afectados o mínimamente afectados.
- Áreas a informar: Se dará conocimiento a la Gerencia de TI. Se informará a la Gerencia General y Consejo de Administración solo en caso de que se vean afectados servicios utilizados por los socios de Universitaria.
- Periodos de permanencia fuera de servicio: En caso que algún servicio que afecte a los Socios quedara sin funcionar, por el mantenimiento se informará previamente a la Gerencia General y/o Consejo de Administración el periodo en que los servicios estarían abajo.

Equipos de red (switches y routers)

- Período de Mantenimiento: Realizar el mantenimiento preventivo de Switches, routers y equipos activos por lo menos una vez al año, tanto para Casa Matriz como Sucursales.
- Días y Horarios: El mantenimiento debería ser realizado en días y horarios en los que los servicios ofrecidos a los socios y/o procesos no se vean afectados o bien mínimamente afectados en casos en que los servicios sean de 24 horas.
- Áreas a informar: Se dará conocimiento a la Gerencia de TI. Se informará a la Gerencia General y Consejo de Administración solo en caso de que se vean afectados servicios utilizados por los socios de la cooperativa. En caso de equipos de Sucursales se deberá coordinar con el Subgerente de la sucursal afectada.
- Periodos de permanencia fuera de servicio: En caso que algún servicio que afecte a los Socios quedara sin funcionar, por el mantenimiento se informará previamente a la Gerencia General y/o Consejo de Administración el periodo en que los servicios estarían abajo.

Equipos de Aire Acondicionado de Sala de Servidores (Matriz)

- Período de Mantenimiento: La verificación y el mantenimiento preventivo de Aire Acondicionado de Sala de Servidores de Casa Matriz se deberá realizar cada mes **o cada 6 meses** por técnicos externos a la Universitaria en coordinación con el área de Redes y/o Base de Datos de TI.
- Días y Horarios: El mantenimiento preventivo de Aire Acondicionado se realizará en cualquier momento siempre y cuando no afecte el desempeño normal de los equipos dentro de la Sala de Servidores.
- Áreas a informar Se dará conocimiento a la Gerencia de TI. Se informará a la Gerencia General y Consejo de Administración solo en caso de que se vean afectados los servicios utilizados por los socios de Universitaria.

CAPITULO VIII. PROCESO DE CIERRE DIARIO

1. Disposiciones generales:

Cierre diario.

a) Se da inicio al cierre informático al finalizar la jornada laboral (19:00 hs. en adelante), con los cierres de cajas de las sucursales y los procesos de débitos automáticos concluidos.

b) Los datos del cierre serán registrados en el sistema informático, a fin de contar con un mecanismo de control, que permita realizar las verificaciones que sean necesarias.

Procesos diarios del Dpto. de Operaciones de Tarjetas de Crédito.

El Departamento de Operaciones de Tarjetas de Crédito, será responsable de la verificación y confirmación de los saldos actualizados de las tarjetas, posterior al proceso de actualización de datos realizado por el RPA (Robotic Process Automation).

Proceso	Descripción	Horario
Actualización de tarjetas.	El RPA (Robotic Process Automation) es el encargado de descargar los archivos de las entidades de Panal, Cabal y Máster, depositarlos en los servidores correspondientes, actualizar los saldos. El resultado es la actualización de saldos de tarjetas de crédito para el extracto general del socio.	Lunes a Viernes 06:00 a 8:00 hs. Sábados 06:00 a 08:00 hs.

Procesos diarios del Dpto. de Operaciones de Base de Datos.

El Departamento de Operaciones de base de datos cuenta con las siguientes responsabilidades

PROCESOS DE ACTUALIZACION DE TARJETAS		
Proceso	**Descripción**	**Horario**
Verificación de tarjetas.	El RPA realiza la descargar de los archivos para la actualización de tarjetas en el sistema.	Lunes – Viernes 06:00– 8:00 hs. Sábados 06:00 - 8:00 hs.
Bajar archivos de *Pronet*, *Netel, Documenta, Infonet*.	Se realizan las descargas de los archivos para las conciliaciones, el proceso de actualización se realiza en el programa CONA4000.	Lunes – Viernes 07:30– 8:00 hs.
	Obs: Los usuarios del Dpto. de Operaciones de Tarjetas cuentan con herramienta para la descargar los mismos archivos.	Lunes – Viernes 07:30– 8:00 hs. Sábados 07:30 - 8:00 hs.

PROCESOS DE CIERRE SEMI-AUTOMÁTICO	
Proceso	**Descripción**
Cierre Semiautomático.	Una vez verificado que todas las cajas se encuentren cerradas y los débitos hayan finalizado, se corre el cierre semiautomático Prog. SCUA1000.
Generación de Archivos de Pagos.	Correr el proceso del programa TARJ016 para la generación de archivos de pagos de las procesadoras.

Los procesos de cierre se correrán todos los días a partir del cierre total en horario de las 19:00hs en adelante, de todas las cajas y procesos de débitos culminado.

CAPITULO IX. UTILIZACION DE LA HERRAMIENTA DE CONTROL DE ESCRITORIO REMOTO

1. **Objetivo**

Establecer las normas inherentes a las conexiones de Control de Escritorio Remoto, en los equipos de los Colaboradores de Universitaria.

2. Disposiciones generales

a) Todos los equipos de la Cooperativa deben contar con el software empleado para el Control de Escritorio, de manera a poder recibir Soporte Técnico en caso de necesidad. Esto no se aplica a los equipos de Gerentes y funcionarios del departamento de Auditoría Interna.

b) Tendrán instalado el modo Administrador para poder conectarse remotamente a los demás equipos, los funcionarios del Departamento de TI y del Departamento de Seguridad TI.

c) En caso de que otro departamento precise la opción de conectarse remotamente a los equipos de la Cooperativa, deberá solicitar autorización al Departamento de Seguridad TI para su aprobación respectiva.

d) Ya sea que el funcionario necesite soporte o se necesite realizar alguna configuración en el equipo, el Operador de TI o Seguridad de TI deberá comunicar telefónicamente al usuario que se realizará una conexión por escritorio remoto al equipo el Usuario. Este deberá dar su conformidad en forma verbal.

e) Todos los equipos de los usuarios deberán tener la opción de “Confirmación Local”, es decir se debe desplegar al usuario un “prompt” indicando que otro equipo quiere conectarse remotamente. Así también el usuario deberá dar su conformidad por este medio. Este punto no es aplicable a las terminales de Autoconsulta.

f) Durante el tiempo que dure la conexión, al funcionario se le desplegará un ícono indicando que otra PC está conectada al Control de Escritorio Remoto.

g) Una vez culminada la tarea en la PC que se controló remotamente, se debe realizar la desconexión de esta y dar aviso al usuario respectivo.

h) En ninguna circunstancia el Operador se podrá conectar a la PC sin la autorización del usuario.

Otras consideraciones.

En caso de implementación de Nuevas Tecnologías (Software y hardware), los responsables de las áreas deberán comunicar vía correo electrónico al Departamento de Seguridad TI, a fin de analizar los riesgos asociados y emitir un parecer técnico para su consideración.