Políticas de Tecnologías de la Información

Contenido

1. Política de Seguridad informática

1.1 Introducción

La seguridad informática ocupa un lugar preponderante en las organizaciones debido al valor intrínseco de la información y su resguardo. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad, lo cual ha traído consigo la aparición de nuevas amenazas para los sistemas de información. Estos riesgos que se enfrentan han llevado a que se desarrolle un documento de directrices que orientan en el uso adecuado de estas tecnologías con el fin de obtener el mayor provecho de estas ventajas y evitar el uso indebido de las mismas, que pueda ocasionar serios problemas a los bienes, servicios y operaciones de la CND.

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

1.2 Alcance

La presente política es elaborada de acuerdo al análisis de riesgos y de vulnerabilidades en las dependencias de CND, por consiguiente, el alcance de estas directrices, se encuentra sujeto a la empresa y alcanza a todos los servicios informáticos, incluyendo la red de comunicaciones.

1.3 Objetivos

Definir claramente la política informática de la institución para cada aspecto relacionado con las Tecnologías de la Información y las Comunicaciones, especificando que se puede utilizar en forma estándar en los equipos de CND así como los procesos a seguir para las excepciones y actualizaciones.

Desarrollar un sistema de seguridad significa "planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la empresa". Los objetivos que se desean alcanzar luego de implantar nuestro sistema de seguridad son los siguientes:

- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de la CND en la administración del riesgo.
- Compromiso de todo el personal de la empresa con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.

- Todos los empleados se convierten en interventores responsables del sistema de seguridad.

1.4 Responsabilidades

Es responsabilidad de la Unidad de Tecnologías de la Información desarrollar y proponer la Política Informática de la institución, así como desarrollar, someter a revisión, capacitar y divulgar los Procedimientos de Seguridad. Asimismo, es responsabilidad del supervisor inmediato verificar que sus empleados ejecuten los Procedimientos de Seguridad.

1.5 Comité de Tecnologías de la Información y las Comunicaciones

El Comité de Tecnologías de la Información y las Comunicaciones (TIC) estará integrado por la Gerencia General, la Gerencia de Administración y Finanzas y el Responsable de la Unidad de Tecnologías de la Información, y podrá contar con asesoramiento externo.

Entre sus cometidos estarán:

- Mantener actualizadas las políticas de seguridad de la información de CND y velar por su cumplimiento.
- Definir estrategias relativas a las adquisiciones de hardware y software.
- Priorizar las tareas y proyectos informáticos, en concordancia con los objetivos estratégicos del CND.
- Definir la Arquitectura tecnológica.
- Realizar el seguimiento de los contratos con proveedores de servicios de TI

El Comité de TIC deberá reunirse como mínimo en forma bimestral. Sus resoluciones deberán documentarse en actas y ser posteriormente elevadas al Directorio de la CND para su conocimiento.

1.6 Definición de directivas informáticas y de seguridad

En esta sección del documento se presenta la política informática y de seguridad, como un recurso para definir los estándares de funcionamiento y de trabajo en materia informática, así como mitigar los riesgos a los que la CND se vea expuesta.

1.6.1 Disposiciones generales

Artículo 1°.- El presente ordenamiento tiene por objeto estandarizar y contribuir al desarrollo informático de las diferentes áreas de la CND.

Artículo 2°.- La Unidad de Tecnologías de la Información será la responsable de:

- Velar por el funcionamiento de la tecnología informática que se utilice en las diferentes áreas.

- Proponer, implantar y efectuar el seguimiento de las políticas informáticas de CND.
- Definir estrategias y objetivos a corto, mediano y largo plazo.
- Mantener la Arquitectura tecnológica.
- Controlar la calidad del servicio brindado.
- Proponer instancias de capacitación en los diferentes aspectos de tecnología de información.
- Mantener el Inventario actualizado de los recursos informáticos:
  - Hardware (PCs, Servidores, Routers, Switches, impresoras, etc.)
  - Software (Microsoft, Autocad, Adobe, Software en general)
- Velar por el cumplimiento de las Políticas y Procedimientos establecidos.

Artículo 3°.- Para los efectos de este documento, se entiende por políticas informáticas al conjunto de reglas obligatorias de aplicación en la institución para todos los usuarios de los servicios informáticos de CND, siendo responsabilidad de la Unidad de Tecnologías de la Información vigilar su estricta observancia en el ámbito de su competencia, tomando las medidas preventivas y correctivas necesarias para que se cumplan.

Artículo 4°.- Las políticas Informáticas son el conjunto de ordenamientos y lineamientos enmarcados en el ámbito jurídico y administrativo de CND, que inciden en la adquisición y el uso de los bienes y servicios Informáticos, las cuales deberán acatarse invariablemente, por aquellas unidades que intervengan directa y/o indirectamente en dichos procesos.

Artículo 5°.- La instancia rectora de los sistemas de informática de la CND es la Unidad de Tecnologías de la Información, y el órgano competente para la definición de este ordenamiento es el Comité de TIC.

Artículo 6°.- Los responsables de cada área en conjunto con la Unidad de Tecnologías de la Información son responsables de vigilar la correcta aplicación de los ordenamientos establecidos por el Comité y demás disposiciones aplicables. (Ver política usuario, propietario, proveedor de servicios)

1.6.2 Términos de referencia para la adquisición de bienes y servicios informáticos

Artículo 7°.- Toda necesidad de tecnología informática se tramitará a través de la Unidad de Tecnologías de la Información.

Artículo 8°.- La Unidad de Tecnologías de la Información, al planear las operaciones relativas a la adquisición de bienes y servicios informáticos según lo previsto en el presupuesto o las excepciones autorizadas, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad, entendiéndose por:

- **Precio:** Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos;
- **Calidad:** Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.

- **Experiencia:** Presencia en el mercado nacional e internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.
- **Desarrollo Tecnológico:** Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.
- **Estándares:** Toda adquisición se basa en los estándares.
- **Capacidad:** Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área y el crecimiento previsto.

Artículo 9°.- Para la adquisición de Hardware se observará lo siguiente:

- El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo.
- Los equipos informáticos deberán tener una garantía mínima de 3 años en el caso de los puestos de trabajo y deberán contar con el servicio técnico correspondiente en el país (pueden existir excepciones en caso de que los representantes no brinden este plazo de garantía en el país).
- La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional y/o internacional, así como con asistencia técnica y soporte técnico local.
- Los dispositivos de almacenamiento, así como las interfaces de entrada/salida, deberán estar acordes con la tecnología vigente, tanto en velocidad de transferencia de datos, como en procesamiento.
- Los equipos adquiridos deben contar, en lo posible con asistencia técnica durante la instalación de los mismos.
- En lo que se refiere a los servidores, equipos de comunicaciones, concentradores de medios y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya eventualmente el suministro de refacciones al vencer su período de garantía, así como un esquema de redundancia que permita una alta tolerancia a fallas y por ende una alta disponibilidad del servicio.

Todo proyecto de adquisición de bienes de informática (hardware y software) debe sujetarse al análisis, aprobación y autorización de la Unidad de Tecnologías de la Información y cumplir con la Política de compras y contrataciones vigente en CND.

Artículo 10°.- En la adquisición de equipo de cómputo se deberá incluir el software vigente precargado con su licencia correspondiente (SO, Paquete de oficina, etc.).

Artículo 11°.- Todos los productos de Software que se utilicen deberán contar con su licencia de uso respectiva.

Artículo 12°.- Para la operación del software de red, en caso de manejar los datos empresariales mediante aplicaciones (sistemas de información), se deberá tener en consideración lo siguiente:

- El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información

institucional. Los niveles de seguridad de acceso deberán controlarse por los administradores de sistemas (el responsable de la Unidad de TI y los técnicos de TI que él asigne) y poder ser manipulado por software.

- Se deberán delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes, en concordancia con la Política de Propietario – Usuario – Proveedor de servicios.
- Los datos de los sistemas de información, deberán ser respaldados de acuerdo a la frecuencia de actualización de sus datos, rotando los dispositivos de respaldo de acuerdo al procedimiento definido por la Unidad de TI. En cuanto a la información de los equipos de cómputo personales, se recomienda a los usuarios que guarden sus datos en las unidades de red que estarán comprendidas en el régimen de respaldo, o en medios de almacenamiento alternos (pendrive o similares) bajo su propia gestión. Dejar constancia de que los PCs no se respaldan. Toda información respaldada que se guarda fuera de la CND deberá ir encriptada. Ver política de respaldos de CND.
- Se deberán implantar rutinas periódicas de auditoría a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

Artículo 13°.- Todo nuevo proyecto que quiera acometer la CND que tenga un componente informático deberá contar con la participación, opinión y aprobación de la Unidad de Tecnologías de la Información, así como deberá disponer del presupuesto necesario para los requerimientos en materia informática y su mantenimiento posterior.

Todo proyecto de contratación de desarrollo o construcción de software requerirá de un estudio de factibilidad que permita establecer la rentabilidad del proyecto así como los beneficios que se obtendrán del mismo. Asimismo deberá contar con la aprobación y priorización del Comité de TIC.

Todo contratación de servicios informáticos que implique la firma de un contrato deberá incluir una cláusula donde se acuerde cuál es el nivel de servicio que CND acepta de los proveedores y este último se compromete a brindar. Para servicios que requieran procesamiento o administración de datos pertenecientes a la CND se deberán incluir:

- Cláusulas donde el proveedor tenga la obligación de reportar a CND incidentes de seguridad que puedan ocurrid de manera oportuna.
- Cláusulas en las que se reserve el derecho a la CND para la realización de auditorías tendientes a verificar el alineamiento y cumplimiento con las políticas de seguridad de la información de CND.

1.6.3 Instalaciones de equipos informáticos

Artículo 14°.- La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados.
- La Unidad de Tecnologías de la Información, deberán contar con un croquis actualizado de las instalaciones de comunicaciones del equipo de cómputo en red.
- Las instalaciones eléctricas y de comunicaciones, estarán fijas y resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el Comité.

1.6.4 Lineamientos en Información

Artículo 15.1°.- La información podrá ser clasificada de la siguiente forma:

- Dato personal: Información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.
- Dato sensible: Datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.
- Información pública: Es toda la información que emana, produce, está en posesión de, o bajo el control de CND, con independencia del soporte en el que esté contenida, salvo las excepciones o secretos establecidos por ley, así como la información reservada o confidencial.
- Información reservada: Aquella cuya difusión pueda:
  - Comprometer la seguridad pública o la defensa nacional.
  - Menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de reservado al Estado uruguayo.
  - Dañar la estabilidad financiera, económica o monetaria del país.
  - Poner en riesgo la vida, la dignidad humana, la seguridad o la salud de cualquier persona.
  - Suponer una pérdida de ventajas competitivas para el sujeto obligado o pueda dañar su proceso de producción.
  - Desproteger descubrimientos científicos, tecnológicos o culturales desarrollados o en poder de los sujetos obligados.
  - Afectar la provisión libre y franca de asesoramientos, opiniones o recomendaciones que formen parte del proceso deliberativo de los sujetos obligados hasta que sea adoptada la decisión respectiva, la cual deberá estar documentada.
- Información confidencial: Se considera información confidencial:
  - Aquella entregada en tal carácter a los sujetos obligados, siempre que:
    - Refiera al patrimonio de la persona.

- Comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos a una persona física o jurídica que pudiera ser útil para un competidor.
- Esté amparada por una cláusula contractual de confidencialidad.

- Los datos personales que requieran previo consentimiento informado (Ley Nº 18.331, Arts. 9 y 10).

- Información privilegiada: Se considera información privilegiada:
  - La información de un emisor – o de los valores que emita – obtenida en razón del cargo o posición, inclusive la transmitida por un cliente en relación a sus propias órdenes pendientes, que no se ha hecho pública y que, de hacerse pública, podría influir sensiblemente sobre la cotización de los valores emitidos o sus derivados.
  - La información que se tiene de las operaciones de transmisión de la titularidad a realizar por un inversionista en el mercado de valores, a fin de obtener ventaja con la negociación de valores.

Artículo 15.2°.- La información reservada, confidencial y/o privilegiada:

- Debe ser protegida contra la divulgación no autorizada a través de cualquier medio físico o electrónico.
- Debe ser explícitamente identificada como tal y debe ser destruida al final de su vida útil (considerando los plazos precaucionales definidos por la empresa).
- En caso de ser necesario imprimirse debe hacerse de acuerdo a un procedimiento que se ajuste a la normativa vigente.

Artículo 15.3°. - Constituye uso indebido de la información privilegiada las acciones que se definen a continuación:

- Revelar o confiar información privilegiada antes de que se divulgue al mercado.
- Recomendar la realización de operaciones con valores sobre los que se tiene información privilegiada.
- Adquirir o enajenar – para sí o para terceros, directa o indirectamente – valores sobre los cuales posea información privilegiada.
- En general, valerse de información privilegiada directa o indirectamente, en beneficio propio o de terceros.

Artículo 16°.- Los Propietarios de la información contenida en cada aplicativo delimitarán las responsabilidades y determinarán quién está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.

Artículo 17°.- La información almacenada en medios magnéticos, de carácter histórico quedará documentada como activos del área y estará debidamente resguardada en su lugar de almacenamiento (Archivo de CND).

Es obligación del responsable del área, la entrega conveniente de la información, a quien le suceda en el cargo.

Artículo 18°.- Los sistemas de información en operación, como los que se desarrollen deberán contar con sus respectivos manuales. Un manual del usuario que describa los procedimientos de operación y el manual técnico que describa su estructura interna, programas, catálogos y archivos.

Artículo 19°.- Ningún colaborador en proyectos de software y/o trabajos específicos podrá utilizar material o información de CND, para usos y/o intereses ajenos a la Institución.

Artículo 20°.- Los Gerentes de área son los responsables de otorgar permisos especiales a determinada información a los usuarios de su sector, solo ellos pueden solicitar al área de Tecnología de la Información los cambios en los permisos, se debe dejar constancia de la solicitud mediante correo electrónico y ticket electrónico (STIT). En caso de que el Gerente se encuentre de licencia el pedido puede ser realizado por el superior inmediato utilizando la misma vía que el Gerente.

Artículo 21°.- Toda salida de información (en soportes informáticos o por correo electrónico) sólo podrá ser efectuada por personal autorizado y únicamente para cumplir con los intereses de la CND. Para la salida de información que responda a intereses ajenos a la CND, será necesaria la autorización formal del responsable del área de la que proviene la información. Se prohíbe expresamente copiar, reproducir, ceder a cualquier título o transferir en forma total o parcial, información, programas, software, etc., sea cual fuere el motivo del retiro, a vía de ejemplo: prestarlos, venderlos, copiarlos, transferirlos a terceros o para su uso personal, sin autorización previa y por escrito.

1.6.5 Funcionamiento de los equipos informáticos

Artículo 22°.- Es obligación de la Unidad de Tecnologías de la Información vigilar que el equipo informático se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.

Artículo 23°.- Por seguridad de los recursos informáticos se deberá establecer seguridad:

- Físicas
- Sistema Operativo
- Software
- Comunicaciones
- Base de Datos
- Proceso
- Aplicaciones

Por ello se establecen los siguientes lineamientos:

- Mantener claves de acceso que permitan el uso solamente al personal autorizado para ello.
- Verificar la información que provenga de fuentes externas a fin de corroborar que esté libre de cualquier agente contaminante o perjudicial para el funcionamiento de los

equipos (cada dispositivo USB que se conecta a la CND debe de ser chequeado por el Antivirus).

- En caso de trabajar con un equipo perteneciente a CND fuera del establecimiento, todos los documentos que contengan información de cualquier índole referente a CND deben ser almacenados en una unidad externa y no en el equipo, este procedimiento es necesario para mantener la seguridad de la información perteneciente a la corporación.

Artículo 24°.- En ningún caso se autorizará la utilización de dispositivos ajenos a los procesos informáticos del área. Por consiguiente, se prohíbe el ingreso y/o instalación de hardware y software particular, es decir que no sea propiedad de CND, excepto en casos emergentes que la Dirección autorice expresamente.

Artículo 25°.- Los dispositivos móviles propiedad de CND que utilizan los colaboradores se regirán por la Política de uso de dispositivos móviles.

1.6.6 Plan de Contingencias Informáticas

Artículo 26°.- La Unidad de Tecnologías de la Información creará para las áreas un plan de contingencias informáticas que incluya al menos los siguientes puntos:

- Continuar con la operación del área con procedimientos informáticos críticos:
  - Gia
  - Servidor de archivos Z:
  - Internet
- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Contar con un mecanismo de contacto al cual se pueda recurrir en el momento en que se detecte cualquier anomalía. El Comité de TIC definirá el horario normal de funcionamiento de la Mesa de Ayuda y definirá los procedimientos y servicios disponibles fuera del horario normal de atención.
- Ejecutar pruebas de la funcionalidad del plan de contingencia.
- Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

1.6.7 Estrategias informáticas

Artículo 27°.- La estrategia informática de CND está orientada hacia los siguientes puntos:

- Funcionamiento de los sistemas en ambiente WEB, independientes del equipamiento utilizado y del navegador.
- Esquemas de operación bajo el concepto multicapas.
- Estandarización de hardware, software base, utilitarios y estructuras de datos.
- Manejo de proyectos conjuntos con las diferentes áreas.
- Programa de capacitación permanente para los colaboradores de la empresa.

Artículo 28°.- Para la elaboración de los proyectos informáticos y para la presupuestación de los mismos, se tomarán en cuentan tanto las necesidades de hardware y software del área

solicitante, como la disponibilidad de recursos con los que cuente la CND. Todo proyecto informático deberá contar con la aprobación y priorización del Comité de TIC.

1.6.8 Acceso físico y remoto

Artículo 29°.- Solo podrán a acceder al Datacenter los miembros de la Unidad de TI; en caso de que otros colaboradores o técnicos externos necesiten acceder al Datacenter deberán hacerlo en compañía de un técnico de la Unidad de TI y dejarlo registrado en la planilla de Visitas del Datacenter.

Artículo 30°.- El acceso remoto a la red de la institución deberá llevarse a cabo solo por motivos específicos, a los recursos requeridos y utilizando la VPN, mediante un mecanismo de doble autenticación. Solo podrán acceder aquellas personas debidamente identificadas y autorizadas por su superior inmediato y por el Responsable de la Unidad de Tecnologías de la Información.

1.6.9 Identificación de usuarios y contraseñas

Artículo 31°.- Todos los usuarios con acceso a un sistema de información o a una red informática, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña. La contraseña deberá cumplir con los siguientes requisitos:

- contener como mínimo 8 caracteres,
- incluir al menos una mayúscula, una minúscula, un número y un carácter especial,
- no se podrán repetir las últimas 6 contraseñas utilizadas,
- tener una vigencia máxima de 120 días y una vigencia mínima de 1 día,
- no podrá contener nombre o apellido del usuario.

Luego de 5 intentos fallidos de acceso el usuario se bloqueará, debiendo comunicarse con la Unidad de TI para su desbloqueo.

Las sesiones de estaciones de trabajo sin actividad luego de un período de 10 minutos deberán desconectarse automáticamente o bloquearse; solicitando el ingreso de la contraseña nuevamente.

Artículo 32°.- Ningún usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Política de Seguridad vigente.

Artículo 33°.- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.

Artículo 34°.- Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

1.6.10 Responsabilidades personales

Artículo 35°.- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado. Se entiende por acceso autorizado, a todo usuario y clave correspondiente a un sistema de CND alojado en el Datacenter o en la nube o a cualquier otro sistema con el cual se interactúe en el ejercicio de sus funciones en CND (por ejemplo: sistemas bancarios, sistemas del BCU, sistemas de AIN, BPS, etc.).

Artículo 36°.- Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

Artículo 37°.- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

Artículo 38°.- Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y este reportar al responsable de la administración de la red.

Artículo 39°.- La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.

Artículo 40°.- En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.

Artículo 41°.- Los usuarios deben cumplir con el deber de confidencialidad respecto de la información obtenida en la Organización, de acuerdo a lo definido en el apartado 1.1.4 de la presente política y a las disposiciones legales vigentes.

Artículo 42°.- Los funcionarios abocados a las tareas de vigilancia con acceso al control de cámaras, deben mantener estricta confidencialidad con la información visual. La información recabada en caso de sucesos extraños o solicitada por el personal a cargo debe ser manipulada con la más alta confidencialidad y profesionalismo, siendo responsable totalmente de su difusión el funcionario encargado de la visualización de cámaras.

Artículo 43°.- Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar la seguridad de la información confidencial: pérdida de listados y/o soportes magnéticos, sospechas de uso indebido del acceso autorizado por otras personas, revelación de la información o utilización para fines ajenos a los laborales, etc.

1.6.11 Uso apropiado de los recursos

Artículo 44°.- Todos los Recursos Informáticos, Datos, Software, Red Corporativa y Sistemas de Comunicación Electrónica (por ejemplo el correo electrónico) son herramientas de trabajo y están disponibles exclusivamente para cumplir las obligaciones y propósitos de la operativa para la que fueron diseñados e implantados. La Organización, en ejercicio de su poder de control y supervisión podrá, en cualquier momento y sin requerir aviso ni notificación previa, acceder a los contenidos de los medios electrónicos puestos a disposición de los usuarios. Todo el personal

que utilice dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso y en la información allí generada y almacenada.

Artículo 45°.- No está permitido el uso de los recursos para actividades no relacionadas con el propósito del trabajo.

Artículo 46°.- No están permitidas las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Hardware/Software o de los Estándares de los Recursos Informáticos propios de CND

Artículo 47°.- No está permitido introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, discriminatorios, inmorales u ofensivos, así como utilizar cualquier recurso informático para generar, almacenar, visualizar o transmitir estos contenidos.

Artículo 48°.- No está permitido introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos. El personal contratado por CND tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

Artículo 49°.- No está permitido intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.

Artículo 50°.- No está permitido albergar datos, documentos e información de carácter personal en las unidades de discos mapeadas al servidor (Ej: Z:\ I:\)

Artículo 51°.- Cualquier fichero introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.

1.6.12 Uso de software

Artículo 52°.- Todo el personal que accede a los Sistemas de Información de CND debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

Artículo 53°.- Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados, siendo responsable civil y penalmente de la violación de los derechos de propiedad intelectual, y debiendo mantener indemne a CND de cualquier reclamo vinculado a ese concepto.

Artículo 54°.- También tiene prohibido borrar cualquiera de los programas instalados legalmente.

1.6.13 Controles sobre software malicioso

Artículo 55°.- Los usuarios no deben intentar erradicar del equipo software malicioso, como ser virus, troyanos, gusano, spyware, etc. En caso de sospecharse de una infección se debe apagar el equipo o desconectarlo de la red y llamar a TI en forma inmediata. Además, deberá suspenderse el uso de cualquier dispositivo de almacenamiento utilizado en la computadora infectada.

Artículo 56°.- Todo software, antes de su instalación o ejecución deberá ser revisado a efectos de verificar que se encuentra libre de virus. Si el software está encriptado y/o comprimido deberán verificarse, además, los archivos resultantes de su desencriptación y/o descompresión.

Artículo 57°.- Los archivos provenientes de una fuente externa solo podrán ser utilizados después de haber sido controlados con el software antivirus.

Artículo 58°.- TI será el responsable de seleccionar e implementar como estándar el software antivirus destinado a la protección de las estaciones de trabajo, dispositivos móviles y servidores de la red. Periódicamente se actualizará el estudio realizado.

Artículo 59°.- Todos los equipos informáticos deberán tener instalado y funcionando en las condiciones establecidas el software antivirus seleccionado como estándar. Se prohíbe al usuario la deshabilitación del mismo y la realización de cambios en la configuración, los cuales podrán ser efectuados exclusivamente por TI. Cuando por alguna razón no sea posible instalar software antivirus en un equipo, se deberán adoptar las medidas compensatorias necesarias y suficientes para reducir los riesgos derivados del software malicioso. Asimismo deberán instalarse en todos los equipos informáticos, todas las actualizaciones que el proveedor del software antivirus indique y que mejoren las capacidades del producto.

Artículo 60°.- El software que se distribuya a terceras partes deberá ser sometido, previamente, a pruebas de detección de posibles virus. Deberán documentarse los objetivos, las herramientas utilizadas y los resultados de dichas pruebas.

Artículo 61°.- La Unidad de TI, verificará periódicamente en todos los servidores y todas las estaciones de trabajo que el software antivirus está instalado, funciona en las condiciones establecidas y se encuentra actualizado.

1.6.14 Red Corporativa

Artículo 62°.- No está permitido conectar a ninguno de los Recursos, ningún tipo de equipo de comunicaciones (Ej. módem de comunicaciones 3G) que posibilite la conexión desde y hacia la Red Corporativa desde fuera de esta y los mecanismos de seguridad que brinda.

Artículo 63°.- No está permitido conectarse a la Red Corporativa a través de otros medios que no sean los definidos, así como conectar equipos personales de cualquier índole. Para conectar cualquier tipo de equipamiento personal a la red (por ejemplo portables) se deberá obtener la autorización expresa de la Unidad de Tecnologías de la Información, quién evaluará cada caso en particular y procederá en consulta con el Comité de TICs.

Artículo 64°.- No está permitido intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.

Artículo 65°.- No está permitido intentar acceder a áreas restringidas de los Sistemas de Información o de la Red Corporativa.

Artículo 66°.- No está permitido intentar distorsionar o falsear los registros "log" de los Sistemas de Información.

Artículo 67°.- No está permitido intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

Artículo 68°.- No está permitido poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, ni dañar o alterar los Recursos Informáticos.

1.6.15 Conectividad a internet

Artículo 69°.- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de CND tienen las mismas responsabilidades en cuanto al uso de Internet. Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado

Artículo 70°.- El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con cortafuegos incorporado en la misma. No está permitido acceder a Internet desde un puesto de trabajo de la red llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

Artículo 71°.- En caso de tener que producirse una transmisión de datos importante, confidencial o relevante, sólo se podrán transmitir en forma encriptada (https/ssh, etc).

1.7 Actualizaciones de la política de seguridad

Artículo 72°.- Debido a la propia evolución de la tecnología y las amenazas de seguridad, y a las nuevas aportaciones legales en la materia, CND se reserva el derecho a modificar esta Política cuando sea necesario. Los cambios realizados en esta Política deben ser aprobados por Directorio y divulgados a todos los colaboradores de CND. Por lo tanto la presente política estará vigente hasta tanto no se comuniquen por los medios habituales las modificaciones.

Artículo 73°.- Es responsabilidad de cada uno de los colaboradores de CND la lectura y conocimiento de la Política de Seguridad más reciente.

1.8 Vigencia

Artículo 74°.- Las disposiciones aquí enmarcadas, entrarán en vigor a partir de la aprobación del presente documento.

Artículo 75°.- Las normas y políticas objeto de este documento, podrán ser modificadas por sugerencia del Comité de Tecnologías de la Información y aprobadas por Directorio; una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.

Artículo 76º.- La falta de conocimiento de las normas aquí descritas por parte de los colaboradores no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.

2. Política de usuario – propietario - proveedor de servicios de TI

2.1 Introducción

Esta política establece las acciones y responsabilidades de los usuarios propietarios (usuario responsable por la información o acción dentro de su área) y por otro lado el proveedor de servicio (el responsable por el medio en el cual se maneja la información que utiliza el usuario propietario).

2.2 Alcance

Alcanza a la definición de los nuevos requerimientos o las modificaciones a una aplicación, así como la asignación de permisos, creación de usuarios, baja de usuarios, o cualquier otra actividad relacionada con el ciclo de vida de un sistema informático y sus respectivos perfiles de acceso. Es esencial destacar el hecho de que no será responsabilidad de Unidad de Tecnologías de la Información la evaluación y control de las solicitudes relacionadas con las aplicaciones sino únicamente su implementación.

2.3 Marco de actuación

Aplicar la normativa "PROPIETARIO-USUARIO-PROVEEDOR DE SERVICIOS", en base a los siguientes criterios:

a) Las Gerencias deberán cumplir el rol de propietarios de sus respectivos aplicativos:
   - Serán propietarios y responsables de la lógica de funcionamiento de los procesos informáticos que se ejecuten en el ámbito de sus respectivas Gerencias. Serán además propietarios y responsables de los datos que por razones de competencia sean originados y actualizados en el marco de su jurisdicción.
   - Los funcionarios en general serán usuarios de los procesos y los datos, cuando por razones funcionales se requiera el acceso a la ejecución de los procesos y/o la visualización de los datos con la previa autorización del propietario de los mismos.

b) La Unidad de Tecnologías de la Información habrá de cumplir el rol de proveedor del servicio informático y custodio del equipamiento informático, procesos y datos de toda la Organización.

c) Auditoría Interna podrá acceder a consultar cualquier información contenida en las diversas aplicaciones de CND solicitando estos accesos a la Unidad de Tecnologías de la Información que le proporcionará los permisos pertinentes para cumplir los cometidos que le son propios.

2.4 Responsabilidades de los roles establecidos

2.4.1 Propietario de los procesos y datos

Es responsabilidad del propietario de los procesos y datos:

- Especificar los requerimientos de mejora y actualización de los procesos que se correspondan con las tareas de su competencia.
- Asegurar que cuando se desarrolle una aplicación la misma satisfaga los requerimientos especificados y otorgar la aceptación formal de la misma al ser puesta en producción.
- Minimizar el acceso, manipulación y extracción de datos por mecanismos ajenos a los provistos por la propia aplicación desarrollada o adquirida para ese fin (se incluyen en esta categoría las actualizaciones manuales de base de datos, estadísticas o reportes generados con herramientas de ofimática accediendo directamente a los datos, etc). Si fuese necesaria cualquier intervención de los técnicos informáticos para modificar manualmente los datos de las aplicaciones, deberán remitir previamente la autorización expresa en tal sentido.
- Autorizar a usuarios a desarrollar funciones a través de procesos de su propiedad, especificando clara y unívocamente los permisos de acceso a otorgar y/o a denegar.
- Especificar los controles que el proceso y los datos requieren.
- Tomar todas las medidas que estén a su alcance, para asegurar la debida integridad, disponibilidad, exactitud y confidencialidad de los datos.
- Determinar los requerimientos de continuidad de la función que su repartición cumple.
- Asegurar que los usuarios sean adecuadamente entrenados en el uso del sistema.
- Determinar los permisos de acceso al sistema de los usuarios.

2.4.2 Usuario de procesos y datos

Es responsabilidad del usuario de procesos y datos:

- Proteger en forma física y lógica el equipamiento informático que le fuera asignado para su uso.
- Mantener controles apropiados sobre las áreas de contacto con los sistemas de la organización, a saber:
  - el acceso a los mismos,
  - el ingreso de datos,
  - las salidas producidas (digitalizadas, papel o de cualquier índole)
- Reportar al proveedor de servicios y al propietario.
- Cumplir con los requerimientos de seguridad de la información vigentes en la Institución.

2.4.3 Proveedor del servicio

Es responsabilidad del proveedor del servicio:

- Asegurar la disponibilidad de las aplicaciones y datos de la organización de acuerdo a las pautas de funcionamiento acordadas con los propietarios de cada proceso.
- Asegurar que en caso de falla, todos los procesos puedan ser restaurados a la brevedad, con el menor impacto posible para la Institución y de acuerdo al plan de contingencias y de recuperación de desastres establecido.
- Velar por mantener un adecuado nivel de servicio para toda la Organización en relación a la capacidad de los servidores de aplicaciones y datos.
- Implementar un programa de seguridad de la información en la Organización que supone la permanente actualización y seguimiento de las medidas preventivas, de detección y correctivas para proveer un adecuado nivel de seguridad.

2.5 Implantación de la política

La implantación de la política requerirá que las distintas gerencias definan su situación en relación al rol de propietario, usuario o proveedor del servicio según fuera el caso y asegurando que el personal a su cargo interprete y ejecute adecuadamente las tareas encomendadas. En ese sentido una vez aprobada por el Directorio, la política deberá ser comunicada a toda la organización.

La tarea de implantación deberá ser supervisada por la Unidad de Tecnologías de la Información que verificará el adecuado apego a la política establecida y asesorará al Comité de TIC en la eventualidad de que existieran casos confusos de responsabilidad o jurisdicción que requieran una mayor especificación o claridad en las pautas establecidas.

La Unidad de Tecnologías de la Información también tendrá a su cargo la definición de los procedimientos administrativos, con su correspondiente soporte en papel o electrónico, para la correcta documentación y transmisión de los requerimientos y especificaciones establecidos por cada rol (p.ej.: solicitudes de altas, bajas o modificaciones de usuarios y permisos).

Se desprende entonces del punto anterior, que las solicitudes de mantenimiento de las aplicaciones, así como de los perfiles de usuario deberán ser validadas en relación al esquema PROPIETARIO-USUARIO-PROVEEDOR DEL SERVICIO, para asegurar de esta forma los derechos del propietario, y así evitar la definición de USUARIOS de determinados procesos o datos sin previa autorización del PROPIETARIO.

En consecuencia, queda claro que quien centralice la recepción y evaluación de solicitudes de mantenimiento y mejoras de las aplicaciones, así como las altas, bajas y modificaciones de usuarios y permisos de acceso deberá regirse en armonía con la Política aprobada por la Organización.

Ante una solicitud, el responsable del control deberá como mínimo identificar a los propietarios de procesos y datos, y obtener su aprobación para realizar cualquier cambio en el sistema de control de acceso a los procesos y datos del que es responsable, aún cuando el solicitante sea un jerarca de la institución, con excepción de Auditoría Interna, quien podrá solicitar directamente a la Unidad de Tecnologías de la Información los accesos de consulta de la información que considere necesarios para la ejecución de sus funciones.

Otro aspecto de suma importancia en cuanto a los usuarios del sistema y sus permisos de acceso, es la conveniencia de generar únicamente cuentas en el sistema para aquellos usuarios que realmente hacen uso del mismo, y permisos de acceso acordes a sus necesidades y no a su "rango" o posición dentro de la organización. La política en este caso deberá ajustarse a "necesidad de saber, capacidad de hacer", e incluso en algunos mandos superiores, aunque exista la "necesidad de saber", sería conveniente evaluar si esta tarea ha de realizarse por la misma persona o si será delegada a subalternos. Lo que se trata de evitar es la existencia de usuarios con privilegios de acceso que no sean utilizados, pero que representan posibles "puertas de entrada" al sistema para quien decida hacerlo con fines dolosos o propósitos ajenos a los objetivos de la institución. Este tipo de política puede ser incorporada a las observaciones antes mencionadas sobre los controles que deberán realizarse en la administración de usuarios y perfiles.

3. Política de respaldos

3.1 Introducción

La presente política establece las acciones a realizar en CND para asegurar el respaldo de la información, tanto de los sistemas como de los usuarios. Se establece la frecuencia y medios de los respaldos, así como los responsables.

3.2 Alcance

La política alcanza a los respaldos de los archivos de las carpetas en servidores destinadas a tal fin y que son utilizadas por los diferentes usuarios de CND; bases de datos de sistemas corporativos y los respaldos de las máquinas destinadas a los Gerentes de CND.

3.3 Ambientes de datos

CND cuenta con 4 ambientes de datos, que se detallan a continuación:

- Ambiente 1 - Producción: los datos se encuentran almacenados en un Storage configurado como RAID 5[1] lo que brinda una ambiente redundante ante falla de discos.
- Ambiente 2 - NAS[2] en Datacenter: guarda los datos de respaldos diarios por 10 días hábiles.
- Ambiente 3 - NAS en Edificio Rincón 518: guarda los datos de respaldos diarios por 20 días hábiles.
- Ambiente 4 - Discos USB: guarda respaldos semanales por 1 año en la bóveda de un proveedor especializado. Al cabo de 1 año estos discos se trasladan al archivo de CND y permanecen almacenados indefinidamente. Estos respaldos salen de CND por lo tanto están encriptados.

3.4 Respaldo de bases de datos de sistemas corporativos

Las Bases de Datos de los sistemas corporativos se respaldan una vez por día mediante la herramienta de BackUp de SQL Server, este proceso se ejecuta fuera del horario laboral. Estos respaldos son copiados por un sistema especializado de respaldos a los ambientes 2 y 3, fuera del horario laboral de cada día hábil.

---

[1] *RAID 5: sistema de almacenamiento de datos que utiliza múltiples unidades (discos duros o SSD), entre las cuales se distribuyen o replican los datos.*

[2] *NAS (Network Attached Storage): tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un servidor con servidores clientes a través de una red (TCP/IP).*

3.5 Respaldo de servidor de archivos

Los archivos que los usuarios guarden en las carpetas del servidor FileServer serán respaldados según la siguiente frecuencia:

- Respaldo incremental: todos los días en ambientes 2 y 3.
- Respaldo semanal: los jueves en ambiente 4. El respaldo semanal se guarda el primer año en bóveda de un proveedor especializado y al siguiente año en bóveda de CND de manera indefinida.

Los usuarios ven estos archivos como la unidad Z: o unidad E: de su máquina.

3.6 Respaldo de PC de Gerentes

A los gerentes de CND se les entrega un disco duro portátil para que cada uno pueda respaldar la información que considere de sus máquinas, como por ejemplo: pst (archivos de datos de correo), documentos varios que no guarda en la unidad compartida, etc. En este caso cada persona es responsable de realizar los respaldos que considere necesarios y de mantener el disco duro portátil en un lugar seguro.

4. Política de uso de dispositivos móviles

4.1 Introducción

Considerando que CND en la ejecución de sus funciones puede requerir la utilización de dispositivos móviles, como laptops, tablets, entre otros, resulta necesario definir políticas de uso de dichos dispositivos a los efectos de resguardar su integridad física y la información que contienen.

4.2 Alcance

La presente política aplica al uso de todos aquellos dispositivos móviles propiedad de CND, excepto teléfonos celulares, que utilicen tanto funcionarios CND como personal contratado.

4.3 Condiciones de uso

Los dispositivos móviles provistos por CND deben utilizarse para actividades de carácter laboral. El usuario debe tener el debido cuidado de la integridad física del dispositivo.

Cuando exista una solicitud de entrega del dispositivo móvil de CND por parte de TI, lo cual puede ser por razones de auditoría, administración o configuración, los usuarios son responsables de entregarlos a TI.

Los usuarios no tienen permitido realizar ni autorizar ningún arreglo o servicio para el dispositivo que tenga asignado.

4.4 Pérdida o robo de dispositivos de CND

Es responsabilidad del usuario tomar las precauciones apropiadas para prevenir cualquier daño, pérdida o robo del dispositivo.

Si el dispositivo está perdido, robado o se sospecha que está comprometido en cualquier sentido, el usuario debe notificar inmediatamente a la Unidad de TI de la situación y realizar la denuncia policial correspondiente. Esta notificación y la denuncia debe tener lugar para poder cancelar cualquier servicio móvil asociado al dispositivo, así como también borrar remotamente la información contenida en la memoria del mismo en la medida de lo posible.

4.5 Aplicaciones y descargas en dispositivos de CND

Todo el software para el dispositivo debe ser provisto e instalado o aprobado por TI.

4.6 Respaldo, administración de archivos, sincronización y antivirus

El software necesario para realizar respaldos, sincronización de datos y de contactos será proporcionado y/o autorizado por TI.

Es responsabilidad del usuario:

- Realizar los respaldos de la información contenida en el dispositivo.
- Notificar a TI cuando detecte un incorrecto funcionamiento del antivirus o ante sospecha de desactivación u otra anomalía.

4.7 Funcionalidades y características de manejo

El Hardware, sistema operativo y utilitarios que vienen instalados de fábrica y forman parte del dispositivo no deben sufrir cambios a menos que hayan sido requeridos y autorizados por TI. No está permitido que el usuario realice el desbloqueo de las limitaciones del fabricante y/o proveedor (root/jailbreak), ni que realice cualquier otro método de cambio de las protecciones.

4.8 Obligaciones de Seguridad y Privacidad para los datos de la empresa

Los usuarios deben tomar las apropiadas precauciones para prevenir que otras personas externas a la organización (familia, amigos, etc.) tengan acceso a los dispositivos móviles de CND y los recursos asociados a los mismos. Los usuarios no deben:

- Compartir el dispositivo.
- Compartir usuario, contraseña, PIN u otro tipo de credencial.
- Compartir medios de comunicación.

4.9 Buenas prácticas para la protección de los datos

Los usuarios de dispositivos móviles deben cumplir con las políticas de seguridad tanto cuando los usen en el puesto de trabajo como cuando estén fuera de la empresa.

Las instalaciones no gestionadas o no aprobadas comprometen el ambiente operativo y también constituyen un riesgo de seguridad, incluyendo el esparcimiento de virus o software malicioso tanto con o sin intención.

Los usuarios deben respetar las siguientes medidas preventivas de seguridad para proteger la información y las aplicaciones instaladas en el dispositivo:

- Los dispositivos no deben quedar a la vista en un vehículo desatendido, aunque sea por un período corto de tiempo.

- Si en la pantalla de un dispositivo móvil se está mostrando información sensible en un lugar público se debe posicionar de tal manera que la información no pueda ser vista por otros.
- En situaciones vulnerables (aeropuertos, hoteles, centro de conferencias, etc.) el dispositivo no debe quedar desatendido bajo ninguna circunstancia.
- No se debe mover información desde un dispositivo a otro usando bluetooth.
- Solo está permitido copiar información sensible o confidencial al dispositivo móvil o de almacenamiento extraíble cuando sea requerida para trabajar en modo desconectado.
- Para asegurar un almacenamiento adecuado se debe mantener la copia de datos al mínimo, sólo los datos o contenido que sea necesario para propósitos laborales.

4.10 Responsabilidades

Es responsabilidad del Gerente de cada área autorizar el uso de dispositivos móviles de CND a su personal.

La unidad de TI es responsable de:

- La identificación e inventario de los dispositivos móviles como propiedad de CND en forma visible. Dicha identificación deberá ser resistente a su remoción.
- Establecer las condiciones de uso de los dispositivos móviles y comunicar las mismas a los responsables identificados en el inventario.
- Proveer el software necesario para realizar respaldos, sincronización de datos y de contactos, así como también el antivirus necesario para la protección de los dispositivos.
- Garantizar que las tecnologías, aplicaciones y medios de comunicación utilizados sean seguros y confiables.
- Asegurar que las aplicaciones para dispositivos móviles estén disponibles y optimizadas.
- Determinar las medidas de seguridad mínimas que deben tener los equipos a adquirir.

El área responsable de realizar el proceso de adquisición y recepción de dispositivos móviles de uso operativo específico, deberá coordinar con TI para inventariarlo y para el registro de su entrega al destinatario. En oportunidad de la entrega del dispositivo al usuario, la Unidad de TI le proporcionará el documento de políticas de uso de dispositivos móviles y requerirá la firma de un recibo que respalde la entrega del dispositivo y en el cual el usuario declare conocer las políticas que regulan su uso.

En caso de ser posible, los equipos contarán con al menos las siguientes medidas de seguridad:

- Bloqueo de operación mediante contraseña o patrón.
- Encriptación de archivos con información confidencial o reservada.
- Antivirus habilitado y actualizado.

No es responsabilidad de TI recuperar ningún tipo de información en caso de que el dispositivo se haya perdido, haya sido robado o dañado.

Es responsabilidad de los usuarios de dispositivos móviles de CND:

- El cumplimiento de las condiciones de uso establecidas por la Unidad de TI en lo relativo al hardware y al software en él instalado, tanto cuando estos sean utilizados dentro como fuera de la Empresa.
- Llevar el dispositivo a la Unidad de TI cuando sea solicitado por esta, ya sea por razones de auditoría, administración o configuración.
- Tener el debido cuidado de la integridad física del dispositivo.
- Tomar las precauciones apropiadas para prevenir cualquier daño, pérdida o robo del dispositivo.
- En caso de pérdida o robo, el usuario deberá notificar inmediatamente a la Unidad de TI de la situación y realizar la denuncia policial correspondiente.
- Realizar los respaldos y verificar que el antivirus se encuentre activo y actualizado.
- Evitar el bloqueo de las limitaciones del fabricante y/o proveedor (root/jailbreak), o realizar cualquier otro método de cambio de las protecciones con las que se entregó el dispositivo.