Administración de Recursos

Universidad Tecnológica Nacional

# Trabajo de Auditoría

Organización:

Diario

****

Bracamonte, Federico

Cabrera, Cristian

García, Gabriel

Sastre, Yamila

# Manual de Políticas y Estándares de Seguridad Informática

# Diario UNO

# Introducción

La base para que cualquier organización pueda operar de una forma confiable en materia de

Seguridad Informática comienza con la definición de las políticas y estándares.

En éste informe vamos a desarrollar diversos aspectos que consideramos relevantes a la hora de mantener la seguridad de los datos de la empresa (como recurso estratégico fundamental).

La Seguridad Informática, es una función en la que se deben evaluar y administrar los riesgos,

Los puntos a tener en cuenta son los siguientes:

* Seguridad del Personal.
* Seguridad Física y Ambiental.
* Administración de Operaciones de Cómputo.
* Controles de Acceso Lógico.
* Cumplimiento.

## 1.- Disposiciones Generales

### 1.1 Ámbito de aplicación y Fines

Las políticas y estándares de Seguridad Informática definidas tienen por objeto establecer medidas técnicas y de organización de las tecnologías de información y de las personas que interactúan haciendo uso de los servicios informáticos que proporciona el diario UNO y contribuyendo con la función informática a la mejora y complimiento de metas institucionales. Es aplicable a los usuarios de servicios de tecnologías de información adscritos la Coordinación General Administrativa de igual forma es una herramienta que: Difunde las políticas y estándares de seguridad informática a todo el personal del diario UNO

Asegurara: Mayor integridad, confidencialidad y confiabilidad de la información generada por el diario UNO al personal, los datos y el hardware y software disponibles;

Minimiza: los riesgos en el uso de las tecnologías de información

### 1.2 Frecuencia de Evaluación de las Políticas

Las políticas tendrán una revisión semestral para efectuar, actualizaciones, adecuaciones y/o modificaciones basadas en la experiencia.

### 1.3 Beneficios

Las políticas y estándares de seguridad informática establecidas dentro de este documento son a base para la protección de los activos tecnológicos e información del diario UNO.

## 2.- POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política

Todo usuario de bienes y servicios informáticos al ingresar como personal del diario UNO acepta las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información del diario UNO, así como el estricto apego al Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

Los usuarios deberán cumplir con lo establecido en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

### 2.1.1 Usuarios Nuevos

Todo el personal nuevo del diario UNO, deberá ser notificado ante el área de Sistemas y Técnica para dar los derechos correspondientes (Reloj Checador, Equipo de cómputo, Derechos en servidor, solicitud de institucional) o en caso de baja retirar los derechos.

### 2.1.2 Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.

### 2.2 Entrenamiento en seguridad informática

Todo empleado del diario UNO de nuevo ingreso deberá contar con la inducción sobre el “Manual de Políticas y Estándares de Seguridad Informática”, donde se den a conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento.

### 2.3 Medidas disciplinarias

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta dependencia, o de que se le declare culpable de un delito informático.

## 3.- POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Política

Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas del diario UNO sólo a personas autorizadas para salvaguardar los equipos de cómputo y de comunicaciones.

### 3.1 Resguardo y protección de la información

3.1.1 El usuario deberá reportar de forma inmediata al Área de Sistemas cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, principios de incendio u otros.

3.1.2 El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

3.1.3 Es responsabilidad del usuario evitar en todo momento la fuga de la información del diario UNO que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

3.1.3 Es responsabilidad del usuario designado para tal fin, verificar que se lleven a cabo las copias de seguridad designadas por el Área de Sistemas y Seguridad (en tiempo y forma).

### 3.2 Controles de acceso físico

3.2.1 Cualquier persona que tenga acceso a las instalaciones del diario UNO, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad del diario UNO, en el área de recepción, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

3.2.2 Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá salir de las instalaciones del diario UNO únicamente con la autorización de salida del área de Inventarios anexando el formulario de salida del equipo (debidamente completado por el secretario de la oficina o la equivalente en las dependencias del diario UNO).

3.2.3 Los Estacionamientos estarán monitoreados mediante cámaras IP.

### 3.3 Seguridad en áreas de trabajo

3.3.1 Los centros de cómputo del diario UNO son áreas restringidas, por lo que sólo el personal autorizado por el Área de Sistemas y Calidad puede acceder a él.

3.3.2 El ingreso a las áreas de Expedición y Estacionamientos también estará restringido sólo a personal y terceros autorizados, debiendo quedar completamente registrado el ingreso/egreso de los mismos a las instalaciones (registrando hora, propósito, y demás datos pedidos por el sistema de Expedición u Estacionamientos).

### 3.4 Protección y ubicación de los equipos

3.4.1 Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Área de Sistemas y Calidad, en caso de requerir este servicio deberá solicitarlo.

3.4.2 El Área de Inventarios será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el Sistemas y Técnica.

3.4.3 El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones del diario UNO.

3.4.4 Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

3.4.5 Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro en el servidor o en mis “Mis Documentos” ya que las otras están destinadas para archivos de programa y sistema operativo.

3.4.6 Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

3.4.7 Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU.

3.4.8 Se debe mantener el equipo informático en un entorno limpio y sin humedad.

3.4.9 El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reacomodo de cables con el personal de Sistemas y Calidad.

3.4.10 Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación al área de Sistemas y Calidad a través de un plan detallado.

3.4.11 Queda prohibido que el usuario abra o desarme los equipos de cómputo.

### 3.5 Mantenimiento de equipo

3.5.1 Únicamente el personal autorizado por el Área de Sistemas y Calidad podrá llevar a cabo los servicios y reparaciones al equipo informático.

3.5.2 Los usuarios deberán asegurarse de respaldar en el servidor la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

### 3.6 Pérdida de Equipo

3.6.1 El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

3.6.2 El préstamo de laptops tendrá que solicitarse en el Área de Sistemas y Calidad, con el visto bueno del Secretario de la oficina del diario UNO o su equivalente en las dependencias de la Coordinación.

3.6.3 El usuario deberá dar aviso inmediato al Área de Sistemas y Calidad, e Inventarios de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

### 3.7 Uso de dispositivos especiales

3.7.1 El uso de los grabadores de discos compactos es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

3.7.2 El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

3.7.3 Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el Área de Tecnologías de la Información.

### 3.8 Daño del equipo

3.8.1 El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, se levantara un reporte de incumplimiento de políticas de seguridad.

## 4.- POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Política

Los usuarios deberán proteger la información que reside y utiliza la infraestructura tecnológica del diario UNO. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna del diario UNO o hacia redes externas como Internet.

Los usuarios del diario UNO que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

### 4.1 Uso de medios de almacenamiento

4.1.1 Los usuarios de informática del diario UNO deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

4.1.2 Las actividades que realicen los usuarios en la infraestructura de Tecnología de Información del diario UNO son registradas y susceptibles de auditoría.

### 4.2 Instalación de software.

4.2.1 Los usuarios que requieran la instalación de software que no sea propiedad del diario UNO, deberán justificar su uso y solicitar su autorización por el Área de Sistemas y Calidad indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación.

4.2.2 Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red del diario UNO, que no esté autorizado por el Área de Sistemas y Calidad.

### 4.3 Identificación del incidente

4.3.1 El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo al Área de Sistemas y Calidad lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad Informática.

4.3.2 Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar al Área de Tecnologías de la Información.

4.3.3 Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del diario UNO debe ser reportado al Sistemas y Calidad de la Información.

### 4.4 Administración de la configuración

4.4.1 Los usuarios de las áreas del diario UNO no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros quipos de cómputo utilizando el protocolo de transferencia de archivos (FTP, SSH), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del diario UNO, sin la autorización del Área de Sistemas y Calidad.

### 4.5 Seguridad para la red

4.5.1 Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el Área de Sistemas y Calidad, en la cual los usuarios realicen la exploración de los recursos informáticos en la red del diario UNO, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

### 4.6 Uso del Correo electrónico

4.6.1 Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al diario UNO, a menos que cuente con la autorización del Área de Sistemas y Calidad.

4.6.2 Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del diario UNO. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

4.6.3 Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptada y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones

4.6.4 Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

4.6.5 Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

4.7 Controles contra código malicioso

4.7.1 Para prevenir infecciones por virus informático, los usuarios del diario UNO no deben hacer uso de software que no haya sido proporcionado y validado por el Área de Tecnologías de la Información.

4.7.2 Los usuarios del diario UNO deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el Área de Sistemas y Calidad.

4.7.3 Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

4.7.4 Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Área de Sistemas y Calidad.

4.7.5 Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al Área de Sistemas y Calidad para la detección y erradicación del virus.

4.7.6 Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el diario UNO en: Antivirus, Outlook, office, Navegadores u otros programas.

4.7.7 Debido a que algunos virus son extremadamente complejos, ningún usuario del diario UNO debe intentar erradicarlos de las computadoras.

### 4.8 Internet

4.8.1 El acceso a Internet provisto a los usuarios del diario UNO es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

4.8.2 Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por el diario UNO, en caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada por el Área de Sistemas y Calidad.

4.8.3 Los usuarios de Internet del diario UNO tienen que reportar todos los incidentes de seguridad informática al Área de Sistemas y Calidad inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

4.8.4 Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

Serán sujetos de monitoreo de las actividades que realiza en Internet.

Saben que existe la prohibición al acceso de páginas no autorizadas.

Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.

Saben que existe la prohibición de descarga de software sin la autorización del Área de Sistemas y Calidad.

La utilización de Internet es para el desempeño de su función y puesto en el diario UNO y no para propósitos personales.

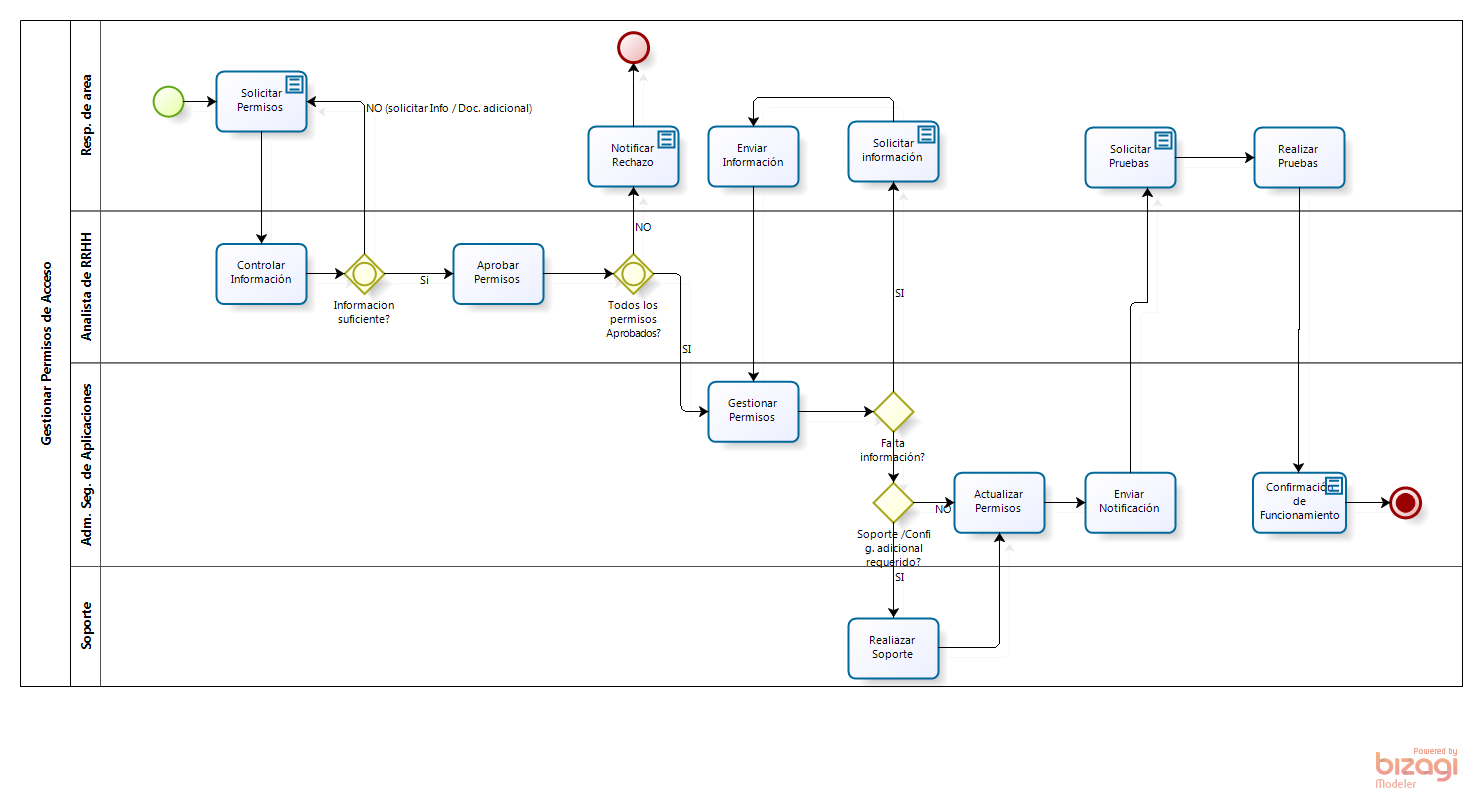
## 5.- POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Cada vez que ingrese un nuevo Empleado en la Organización que tenga acceso a alguna Aplicación Informática para el desarrollo de sus funciones; o que sea necesario - por motivos debidamente justificados - realizar modificaciones de permisos de acceso a Usuarios ya existentes, se deben llevar a cabo los siguientes pasos para gestionar los permisos correspondientes:

1. El Jefe de Área de la persona para la cual se deben generar y/o modificar los permisos de acceso a las aplicaciones debe enviar una solicitud al Analista de RRHH detallando la información “Datos personales” y “Permisos Solicitados”:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| SOLICITUD DE PERMISOS DE ACCESO | | | | | | | |
| **Datos Personales** | | | | | | | |
| **Nombre Persona:** | |  | | | | | |
| **Área:** | |  | | | | | |
| **Función/ Puesto:** | |  | | | | | |
| **Empresa** | |  | | | | | |
| **Nombre de Máquina / IP:** | |  | | | | | |
| **Ubicación física:** | |  | | | | | |
| **{Permisos Solicitados} 1 \*** | | | | | | | |
| **Aplicación** | |  | | | | | |
| **Fecha Inicio** | |  | | | | | |
| **Fecha Fin** | |  | | | | | |
| **Nombre de Usuario:** | | En caso que se cuente con uno. | | | | | |
| **Detalle de permisos:** | | Roles que necesita – funciones a desempeñar. | | | | | |
| **Observaciones** | | Justificación de la solicitud por aplicación. | | | | | |
| **Información de Aprobación** | | | | | | | |
| **Estado Solicitud** | **Aprobada** | | | | **Rechazada** | | |
| **Motivos rechazo** |  | | | | | | |
| **Información de configuración** | | | | | | | |
| **Nombre de ASA** | |  | Fecha realización | | | |  |
| **Nombre de Soporte** | |  | Fecha realización | | | |  |
| **Observaciones** | |  | | | | | |
| **Usuario Final** | |  | | Fecha Confirmación | |  | |

1. El analista de RRHH, una vez recibida la solicitud, debe validar esta información con las funciones correspondientes al puesto que desempeña el Empleado.
   1. Si los permisos solicitados **se condicen** con sus responsabilidades:
      1. Autorizar los mismos, notificando esto al Responsable de área.
      2. Solicitar a Sistemas las tareas necesarias para otorgar los permisos enviando la solicitud correspondiente.
   2. Si los permisos solicitados **no se condicen** con sus responsabilidades:
      1. Solicitar mayor detalle de justificación al solicitante de los permisos ó
      2. Rechaza la solicitud de acceso indicando los motivos correspondientes.
2. El ASA al recibir la solicitud, debe validar los datos informados:
   1. Si falta información, solicitar mayor detalle al Analista de RRHH y/o Resp. de Área.
   2. Solicitar a Soporte, para cada aplicación de la solicitud, el control de los requisitos que debe tener la máquina del usuario para que las aplicaciones funcionen correctamente.
3. El personal de Soporte debe verificar que la máquina del usuario cuente con los requisitos mínimos indicados por el ASA, y en caso de no tenerlos, llevar a cabo la configuración e instalación correspondiente.
4. El ASA, debe completar la información de la solicitud, y confirmar al Analista de RRHH y al originador del pedido, la finalización del procesamiento de la solicitud.
5. El Responsable del Área, este punto, debe solicitarle a su Empleado que lleve a cabo las pruebas necesarias, para controlar que cuenta con los permisos solicitados y que estos funcionan correctamente.
6. El Usuario final, luego de realizar las pruebas correspondientes, para dar por finalizada la solicitud debe informar su conformidad al Responsable de Área, Analista de RRHH, ASA.



Política

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y contraseña necesarios para acceder a la información y a la infraestructura tecnológica del diario UNO, por lo cual deberá mantenerlo de forma confidencial.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica del diario UNO, debe ser proporcionado por el dueño de la información, con base en el principio de la “necesidad de saber” el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

### 5.1 Controles de acceso lógico

5.1.1 Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.

5.1.2 Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Área de Sistemas y Calidad antes de poder usar la infraestructura tecnológica del diario UNO.

5.1.3 Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del diario UNO, a menos que se tenga el visto bueno del dueño de la información y del Área de Tecnologías de la Información y la autorización del secretario de la oficina del diario UNO o su equivalente en las dependencias de la Coordinación.

5.1.4 Cada usuario que acceda a la infraestructura tecnológica del diario UNO debe contar con un identificador de usuario (UserID) único y personalizado. Por lo cual no está permitido el uso de un mismo UserID por varios usuarios.

5.1.5 Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (UserID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tienen prohibido utilizar el UserID de otros usuarios.

### 5.2 Administración de privilegios

5.2.1 Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados a el Área de Sistemas y Calidad, para el cambio de privilegios.

### 5.3 Equipo desatendido

5.3.1 Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados y autorizados por el Área de Tecnologías de la Información cuando no se encuentren en su lugar de trabajo.

### 5.4 Administración y uso de contraseña

5.4.1 La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

5.4.2 Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al Área de Tecnologías de la Información para que se le proporcione una nueva contraseña.

5.4.3 Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

5.4.4 Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar.

Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.

5.4.5 Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, deberá cambiarlo inmediatamente.

5.4.6 Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

### 5.5 Control de accesos remotos

5.5.1 La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del Área de Tecnologías de la Información.

## 6.- POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD

## INFORMÁTICA

Política

El área de Sistemas y Calidad tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

### 6.1 Derechos de propiedad intelectual

6.1.1 Los sistemas desarrollados por personal interno o externo que controle el área de Sistemas y Calidad son propiedad intelectual del diario UNO.

### 6.2 Revisiones del cumplimiento

6.2.1 El área de Sistemas y Calidad realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

6.2.2 El área de Sistemas y Calidad podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la política de Seguridad de Personal.

6.2.3 Los jefes y responsables de los procesos establecidos en el diario UNO deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

### 6.3 Violaciones de seguridad Informática

6.3.1 Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el Área de Tecnologías de la Información.

6.3.2 Ningún usuario del diario UNO debe probar o intentar probar fallas de la Seguridad Informática o conocidas, a menos que estas pruebas sean controladas y aprobadas por el Área de Tecnologías de la Información.

6.3.3 No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del diario UNO.

# Matriz de Riesgos

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo** | **Áreas Afectadas** | **Probabilidad** | **Medidas** |
| **Daño en la fibra óptica que provoca corte del servicio de Internet** | Todas, principalmente el sitio Web | 15% | Poseer al menos un segundo ISP a utilizar en caso de pérdida del enlace principal. Para evitar que ocurra un problema similar con éste ISP, la entrada al edificio será desde el lado contrario del edificio. |
| **Robo de equipos del área de servidores o de racks (discos, routers, switch, modem, servidores)** | Todas | 10% | El acceso al área de servidores o a la habitación del rack está restringido al personal del Área de Sistemas y Calidad, los cuales, para desbloquear la correspondiente puerta, se identifican mediante su huella dactilar. Vigilancia las 24 horas del día y alarmas de monitoreo. |
| **Inundación de la sala de servidores causada por daños en las cañerías del baño cercano (o baños de pisos superiores)** | Todas | 5% | Ubicar los servidores a 1 m. de altura, a salvo de posibles inundaciones. Además equipar la sala con alcantarillas para desagotar rápidamente cualquier fuga de agua. |
| **Corte de energía eléctrica debido a fallas por parte del proveedor** | Todas | 30% | Para cortes de energía de corto tiempo, hay asignadas UPSs para mantener la alimentación de los servidores. Además, se cuenta con generadores eléctricos para cortes prolongados de más de 1 hora. |

# Plan de Contingencias

Objetivos:

* Proteger y conservar los activos de la empresa, ante eventos de riesgos, desastres naturales o actos mal intencionados.
* Reducir la probabilidad de las perdidas, a un mínimo de nivel aceptable, a un costo razonable y asegurar la adecuada recuperación.
* Asegurar que existan controles adecuados para reducir el riesgo por fallas o mal funcionamiento tanto del equipo, como del software, de los datos, y de los medios de almacenamiento.
* Comunicar a todo el personal activo de la empresa los pasos a seguir en caso de cualquier riesgo.

1. **Análisis de Riesgos:**

Se tienen en cuenta dos factores:

1. Los que afectan a la seguridad del edificio.
2. Los que afectan la disponibilidad de los datos.
3. Los que afectan a la seguridad del edificio:

* Inundación de la sala de servidores causada por daños en las cañerías del baño cercano (o baños de pisos superiores).
* Corte de energía eléctrica debido a fallas por parte del proveedor.
* Robo de equipos del área de servidores o de racks (discos, servidores, router, switch, modem).

|  |  |
| --- | --- |
| **Evento** | **Acción** |
| **Inundación de la sala de servidores causada por daños en las cañerías del baño cercano (o baños de pisos superiores)** | Si ocurriera una fuga de agua que provoque una acumulación de 10 cm de ésta en la sala de servidores, las acciones a realizar son:   * Avisar al encargado del mantenimiento de servidores. * Desalojar al personal, si lo hubiere. * Cerrar la alimentación de agua de la fuente del problema. * Si el nivel de agua estuviera por alcanzar los 20 cm, se debe cortar el suministro eléctrico de las áreas inundadas (al menos). * Avisar a Gerente General y departamento de sistemas. * Avisar a mantenimiento para que desagote la sala mediante el uso de una bomba y revise el problema en las alcantarillas que deberían haber evitado la acumulación de agua. * Revisar que no haya agua en la instalación eléctrica antes de restaurar la electricidad (si se hubiera cortado el suministro eléctrico). |
| **Corte de energía eléctrica debido a fallas por parte del proveedor** | Se activara el generador eléctrico. Avisar a mantenimiento o a EDEMSA según gravedad. Comunicar a departamento de sistemas. Notificar a Gerente General. |
| **Robo de equipos del área de servidores o de racks (discos, servidores, router, switch, modem)** | * Comunicar al encargado de seguridad, notificar a la policía, al Gerente General y Gerente de Sistemas. * Determinar los elementos sustraídos y, si no se cuenta con uno de repuesto, comprar uno nuevo. * Si el elemento robado es un router, modem o switch, se debe configurar. * Si el elemento robado es un servidor, se debe realizar la instalación y configuración de las aplicaciones necesarias y la restauración desde el último backup. * Revisar las grabaciones de las cámaras de seguridad para intentar identificar al/los culpable/s y la forma en que se llevó a cabo el robo. |

1. Los que afectan la disponibilidad de los datos:

* Daño en la fibra óptica que provoca corte del servicio de Internet.

|  |  |
| --- | --- |
| **Evento** | **Acción** |
| **Daño en la fibra óptica que provoca corte del servicio de Internet** | * Avisar al departamento de sistemas y de mantenimiento. * Notificar a Gerente General. * Utilizar un dispositivo de Internet móvil hasta que el personal del departamento de mantenimiento pueda reparar los enlaces con los proveedores de Internet principales. |