RESOLUCIÓN No. 100 DE 2018

POR MEDIO DE LA CUAL SE ACTUALIZA
EL MANUAL PARA LA SEGURIDAD DE LA INFORMACIÓN
EN LA INSTITUCIÓN UNIVERSITARIA EAM

EL RECTOR DE LA INSTITUCIÓN UNIVERSITARIA EAM, EN USO DE SUS FACULTADES LEGALES Y ESTATUTARIAS Y

CONSIDERANDO:

Que mediante la Ley 30 de 1992, se organizó el servicio público de la Educación Superior.

Que la INSTITUCIÓN UNIVERSITARIA EAM, es una Institución Privada de Educación Superior, de utilidad común, con código ICFES No. 4709 y personería jurídica reconocida mediante Resolución 032 de julio 31 de 1973 expedida por la Gobernación del Departamento del Quindío.

Que por Resolución Resolución Rectoral No. 090 del 24 de julio de 2014 se adoptó la MANUAL PARA LA SEGURIDAD DE LA INFORMACIÓN en la EAM.

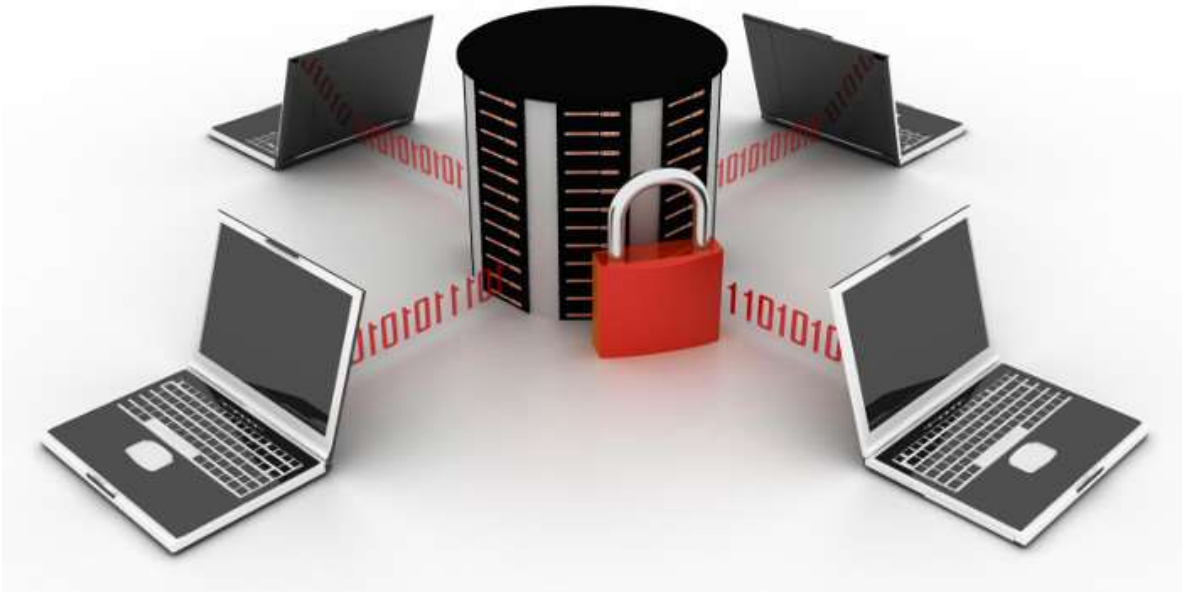
Que teniendo en cuenta la nueva realidad Institucional se hace necesario actualizar la MANUAL PARA LA SEGURIDAD DE LA INFORMACIÓN.

Que de conformidad con el artículo 74 del Estatuto General de la EAM, el Rector es el representante legal de la Institución y se encuentra facultado para la adopción de dicho manual.

RESUELVE:

Artículo Primero. Actualizar el texto del siguiente documento como MANUAL PARA LA SEGURIDAD DE LA INFORMACIÓN en la INSTITUCIÓN UNIVERSITARIA EAM.

MANUAL PARA LA SEGURIDAD DE LA INFORMACIÓN



www.entertic.cat

INSTITUCIÓN UNIVERSITARIA

TABLA DE CONTENIDO

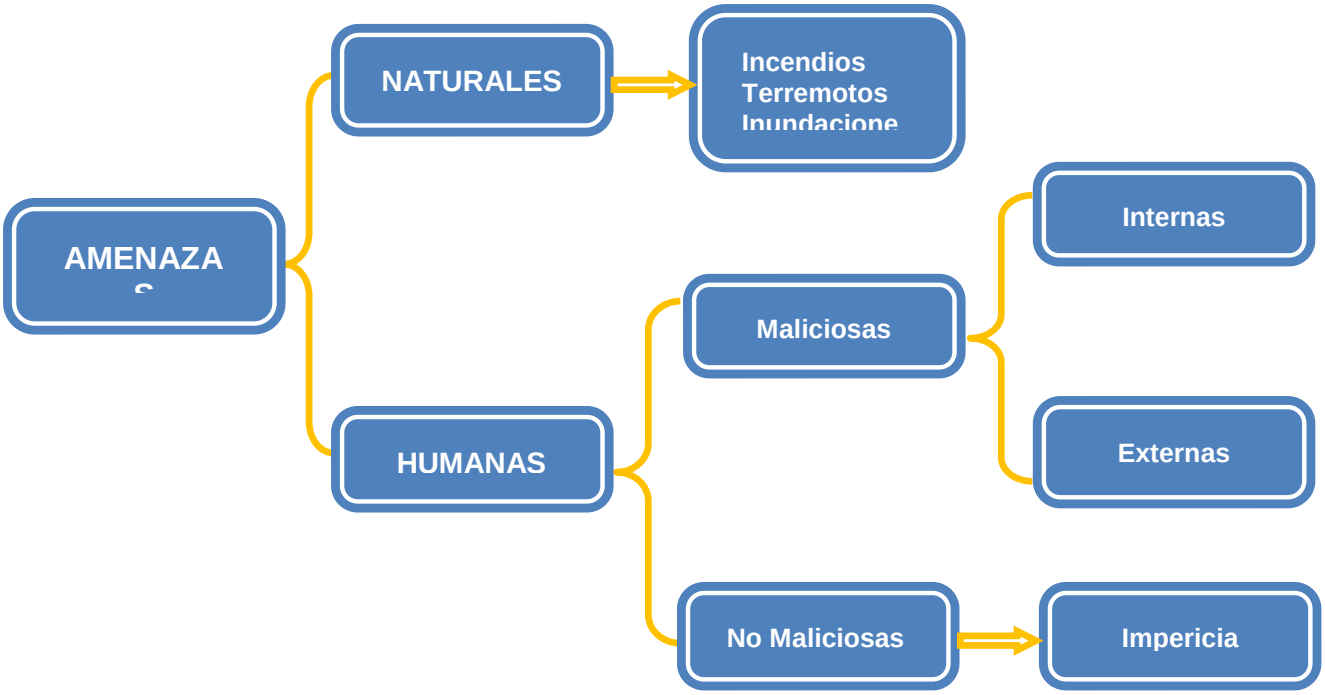
INTRODUCCIÓN

La información es uno de los principales activos de las empresas, razón por la cual tiene un alto valor para las mismas y es crítica para su desempeño y subsistencia. Por tal motivo, al igual que el resto de los activos organizacionales, debe asegurarse que esté debidamente protegida.

Las “buenas prácticas” en Seguridad de la Información, protegen a ésta contra una amplia gama de amenazas, tanto de orden fortuito (destrucción parcial o total por incendio inundaciones, eventos eléctricos y otros) como de orden deliberado, tal como fraude, espionaje, sabotaje, vandalismo, etc.

Una vulnerabilidad es una debilidad en un activo. Una amenaza es una violación potencial de la seguridad. No es necesario que la violación ocurra para que la amenaza exista. Las amenazas “explotan” vulnerabilidades.

La seguridad absoluta no existe en ningún ámbito de la actividad humana. Por ello las medidas de seguridad se diseñan buscando el equilibrio entre su costo, las probabilidades de los distintos riesgos y los daños que estos producirían en caso de materializarse.



La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad**: es garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad**: es salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad**: es garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- **Autenticidad**: es asegurar la validez de la información en tiempo, forma y distribución. Asimismo, garantizar el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Protección a la duplicación**: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- **No repudio**: se refiere a evitar que una persona o entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- **Legalidad**: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- **Confiabilidad de la Información**: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- **Trazabilidad**: característica de la información que asegura el conocimiento de aspectos claves de las operaciones de creación, modificación y consulta, tales como: ¿Quién realizó la operación?, ¿Cuándo se realizó la operación?, ¿Qué resultados tuvo la operación? (Gesdoc).

OBJETIVO

Teniendo en cuenta que las organizaciones a diario están amenazadas por riesgos que ponen en peligro la integridad de la información y con ello la viabilidad de la organización, el objetivo de esta guía es proteger los recursos de información de la INSTITUCIÓN UNIVERSITARIA EAM y la tecnología utilizada para su procesamiento; frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

MARCO NORMATIVO

- ACUERDO No. 047 (05 de mayo de 2000). "Por el cual se desarrolla el artículo 43 del capítulo V "Acceso a los documentos de archivo", del AGN del Reglamento general de archivos sobre "Restricciones por razones de conservación".
- Acuerdo No. 056 (05 de julio de 2000). Por el cual se desarrolla el artículo 45, “Requisitos para la Consulta” del capítulo V, “ACCESO A LOS DOCUMENTOS DE ARCHIVO”, DEL REGLAMENTO GENERAL DE ARCHIVOS.
- Norma ISO 27001:2013:
  - A.6.1.5
  - A.6.2.2
  - A.7.1.3
  - A.9.1
  - A.9.2
  - A.10.4
  - A.10.5
  - A.10.8
  - A.11.2.3
  - A.11.2.4

- LEY 1273 (05 de enero de 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Artículo 269A: Acceso abusivo a un sistema informático
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación
- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269D: Daño Informático.
- Artículo 269E: Uso de software malicioso.
- Artículo 269F: Violación de datos personales.
- Artículo 269G: Suplantación de sitios web para capturar datos personales.

ACUERDOS DE CONFIDENCIALIDAD

actualicese.com

Es recomendable que la EAM establezca acuerdos de confidencialidad con funcionarios y terceros, que reflejen los compromisos de protección y buen uso de la información; donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; dicho acuerdo deberá ser aceptado por cada uno de ellos como parte del proceso de contratación y cualquier violación a lo establecido en el acuerdo de confidencialidad, será considerado como un “incidente de seguridad” (Todo evento que afecte la confidencialidad, como por ejemplo, fallas en los sistemas, pérdida de información y errores por datos incorrecto).

AMENAZAS Y RIESGOS EN EL MANEJO DE LA INFORMACIÓN

Código malicioso (malware)

Es un tipo de software que tiene como objetivo infiltrarse o dañar un computador sin el consentimiento de su propietario, este término se utiliza para referirse a una cantidad de software malicioso, intruso o molesto. Entre ellos encontramos los siguientes:

- Virus: tienen la función de propagarse a través de un software, y su objetivo va desde una simple broma, hasta llegar a realizar daños importantes en los sistemas, o bloquear las redes informáticas.
- Gusanos: tienen la propiedad de duplicarse así mismos, a diferencia de un virus no precisa alterar los archivos de programas, sino que residen en la memoria y casi siempre causan problemas en la red.
- Troyanos: es un software que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero al ejecutarlo ocasiona daños.
- Rootkits: es un programa que permite un acceso de privilegio continuo a un computador, y puede dañar el funcionamiento normal sistema operativo u otras aplicaciones.
- Spyware: es un software que recopila información de un computador y después trasmite esta información a una entidad externa si el conocimiento o el consentimiento del propietario del equipo.
- Keyloggers: son programas maliciosos que monitorizan todas las pulsaciones del teclado y las almacena para un posterior envío al creador.
- Stealers: son sistemas que roban información privada que se encuentra almacenada en el computador.
- Adware: es cualquier programa que automáticamente se ejecuta, mostrando publicidad web, después de instalarlo o mientras se está utilizando la aplicación.
- Crimeware: ha sido diseñado, mediante técnicas de ingeniería social u otras técnicas genéricas de fraude en línea, con el fin de conseguir el robo de identidad para acceder a los datos de usuario de las cuentas en línea de compañía de servicios financieros o compañías de ventas por correo; con el objetivo de obtener los fondos de dichas cuentas, o complementar transacciones no autorizadas por su propietario legítimo.
- Pharming: es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o el de los equipos de los propios

usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otro computador.

- Ransomware: Un ransomware, o "secuestro de datos" en español, es un tipo de programa dañino que restringe el acceso a archivos o dispositivos del usuario y pide un rescate a cambio de quitar esta restricción.

Ingeniería Social

x-web.blogcindario.com recuperacion7.blog

Es una acción social destinada a conseguir información de las personas cercanas a un sistema de información; es el arte de conseguir lo que nos interesa de un tercero por medio de habilidades sociales. Por ejemplo el usuario es persuadido a realizar una acción necesaria para dañar un sistema, como recibir un mensaje que lo lleva a una página web recomendada.

- Smishing: Es un tipo de delito informático o actividad criminal usando técnicas de ingeniería social empelando mensajes de texto dirigidos a los usuarios de telefonía celular, con el fin de robar dinero o adquirir información personal.
- Vishing: Consiste en el envío de un correo electrónico en el cual los delincuentes consiguen detalles de datos bancarios mediante un número telefónico gratuito, en la cual una voz computarizada de aspecto profesional requiere de las víctimas la confirmación de su cuenta bancaria, solicitándoles el número de cuenta, tarjeta, PIN, etc.

- Phishing: Técnica utilizada para captar datos bancarios de los usuarios a través de la utilización de la imagen de la entidad bancaria.

POLÍTICAS DE SEGURIDAD

Uso responsable de los recursos y servicios de información

- Restringir la utilización de programas que no hayan sido instalados y autorizados por el área de sistemas de la EAM.
- Los perfiles de acceso a los sistemas de información deben estar definidos de acuerdo con las funciones y responsabilidades de cada empleado.
- Si se envía información confidencial, esta deberá ser cifrada para proteger la confidencialidad.
- Instalar oportunamente las actualizaciones (parches) de seguridad del sistema operativo de un PC.
- Tener instalado y actualizado un sistema de antivirus y antispyware.
- Instalar y configurar un firewall.
- Se debe evitar brindar información que pueda comprometer la seguridad personal o de los sistemas de información; datos como usuario, contraseña, fecha de nacimiento, nombres de familiares, empresas, números de tarjetas, costumbres, etc. Estos datos pueden ser utilizados para dañar los sistemas y realizar acciones perjudiciales.
- Muchos de los mensajes de texto SMS recibidos anunciando premios, bonos y descuentos son falsos y solo buscan robar dinero o información con fines criminales, evite comunicarse con los teléfonos o sitios web desconocidos.

Uso de correo electrónico

- El correo institucional no se debe utilizar para enviar mensajes en cadenas o chistes, este tipo de correos pueden contener engaños y molestar a los destinatarios.
- La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de la EAM, así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable y sin afectar la productividad.
- El envío masivo de mensajes publicitarios corporativos deberá contar con la aprobación de la Dirección de Comunicaciones. Además, para terceros se

deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia, realizar envío de correo masivo, de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre de la dependencia respectiva y/o Servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la EAM y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
- Evitar abrir correos de procedencia desconocida.

Uso de redes sociales

riskcontrol.com.co

Se debe evitar la publicación de información sensible si el sitio no cuenta con funcionalidades de configuración para la confidencialidad de datos. Antes de aceptar las peticiones de amigos, se debe confirmar que la persona sea la que dice ser.

Seleccionar cuidadosamente las aplicaciones que se instalan en los perfiles, ya que muchas de éstas contiene códigos maliciosos que pueden robar información del perfil.

Políticas de respaldo de datos

www.pcworld.com.

Toda la información sensible, valiosa o crítica, residente en los sistemas de cómputo debe tener respaldo periódicamente. La periodicidad y respaldo de la información debe estar definida de acuerdo con las necesidades de recuperación.

Estas políticas deben ser definidas por el Comité de Gestión Documental.

Copias de seguridad (Backup)

Es la primera y la más importante de las medidas de seguridad. Se deben realizar copias de seguridad de la información crítica de la empresa. Hay distintas formas de organizar las copias, pero una bastante eficiente y segura es tener almacenamiento en la nube y disco por cada día laborable de la semana, de este modo, si la copia más reciente fallara, se puede utilizar otra hecha sólo 24 horas antes. Aunque pueda parecer increíble, el incidente grave que se produce con más frecuencia es la pérdida de información por no haber seguido una política correcta de copias de seguridad.

Antivirus

Tener un antivirus actualizado es una medida básica de seguridad, debe instalarse uno en todos los equipos y mantenerlo actualizado. Teniendo en cuenta, además, que algunos virus aprovechan vulnerabilidades del sistema operativo y para protegerse de ellos hay que instalar las actualizaciones que publica el fabricante (en el caso de *Windows* es aconsejable activar la opción de Actualizaciones Automáticas).

También pueden llegar virus en un correo electrónico, así que debe evitarse abrir mensajes de origen desconocido y eliminarlos lo antes posible de su computador. Estos virus suelen elegir asuntos que despiertan la curiosidad del destinatario. Otro medio de infección es la instalación de plugins, por tal motivo se debe elegir la opción “NO” cuando el sistema le diga que se va a instalar un programa, si no se conoce la procedencia del mismo.

NOTA:
Algunos antivirus gratuitos:
BitDefender
www.bitdefender-es.com
AntiVir
www.free-av.com
Free avast!
www.asw.cz

Anti-espías

Hay programas que se instalan de forma oculta en un computador y pueden enviar a quien los controla la información contenida en el mismo e incluso las contraseñas que se tecleen en él, y también le permiten convertirlo en un *zombie (*Es un ordenador que, sin que su propietario lo sepa, está controlado por un usuario malicioso) y utilizarlo para sus propios fines.

Los programa anti-espías protegen de este *software*, pero se debe desconfiar de aquellos que se ofrezcan sin haberlos buscado expresamente, porque algunos programas desinstalan los espías que encuentran en el equipo sólo para instalar uno propio.

NOTA:
Algunos antispyware gratuitos:
WindowsDefender
www.microsoft.com/spain/
athome/security/spyware/
software/default.mspx
AdAware
www.lavasoftusa.com

Cortafuegos (firewall)

El cortafuego es un elemento informático que analiza la información que entra y sale de un computador o de la red de la empresa. Evita los ataques desde el exterior y, además, permiten detectar los programas espía, ya que avisan de que hay procesos desconocidos intentando enviar información a Internet. Junto con el antivirus es una de las medidas básicas de seguridad para los equipos de cómputo conectados a Internet.

NOTA:
Algunos cortafuegos gratuitos:
ZoneAlarm
download.zonelabs.com
Comodo
www.personalfirewall.comodo.com
En el sitio alerta-antivirus.red.es
puede encontrar más antivirus y
cortafuegos gratuitos.

Correo electrónico no deseado (spam)

Se debe evitar dar la dirección de correo a cualquiera, le ayudará a evitar el spam. Si recibe correo de origen desconocido no lo abra, porque puede introducirle un virus, ni lo conteste, porque si contesta confirma al que lo envió que la dirección es correcta y está activa. Tampoco publique direcciones personales en la web de la institución, utilice mejor direcciones corporativas.

Los programas de correo tienen utilidades para filtrar el spam y también hay programas específicos y empresas especializadas que ofrecen el servicio de filtrar, con un elevado grado de eficacia, el correo que llega a la institución. Y, por supuesto, no envíe propaganda por correo electrónico a quien no le haya autorizado previamente para ello, ya que podrá ser sancionado como spammer por la Agencia de Protección de Datos.

NOTA:
Algunos filtros antispam gratuitos:
G-Lock SpamCombat
www.glocksoft.com/sc
K9
www.keir.net/k9.html
Outlook Security Agent
www.outlooksecurityagen
t.com
SpamFighter
www.spamfighter.com
Spamihilator
www.spamihilator.com
SpamPal
www.spampal.org

Sistemas de alimentación ininterrumpida (SAI)

Para evitar que los procesos en curso se interrumpan bruscamente en caso de corte del suministro eléctrico y para filtrar los "microcortes" y picos de intensidad, que resultan imperceptibles pero que pueden provocar averías en los equipos, es muy aconsejable disponer de sistemas de alimentación ininterrumpida, al menos para los servidores y equipos más importantes.

NOTA:
El tiempo de autonomía depende de la potencia de la unidad y de los equipos conectados. En general es suficiente con unos 10-15 minutos, plazo que permite terminar de forma ordenada los trabajos en curso.

POLÍTICAS DE USO RESPONSABLE DE LAS CUENTAS DE USUARIO Y CONTRASEÑAS

Autenticación

www.servicioalpc.c

Se debe asignar nombres de usuario y contraseñas al personal de la EAM, para que las personas que accedan a los sistemas sean identificadas, es recomendable configurar los computadores de forma que al arrancar soliciten al usuario su nombre y contraseña, y este mismo tratamiento aplicarlo a los diferentes programas que se utilicen. Se debe evitar dejar computadores con libre acceso en la institución.
Las cuentas de usuario y contraseñas son de uso personal e intransferible, por ninguna razón puede prestarlas ni utilizar las de otras personas.
El dueño de la contraseña es responsable de todos los eventos que puedan ser realizados con sus cuentas de usuario.
Se deben elegir contraseñas seguras para evitar posibles suplantaciones.
Se debe registrar al área de sistemas cualquier anomalía o sospecha de violación de las contraseñas de acceso.

Normas para construir una Clave de Acceso

- Evite utilizar palabras comunes ni nombres de fácil deducción por terceros (nombre de mascota)
- Evite vincularlas a una característica personal, (teléfono, D.N.I., placa del automóvil, etc.).
- Absténgase de utilizar terminología técnica conocida *(*admin)
- Combine caracteres alfabéticos, mayúsculas y minúsculas, números, caracteres especiales.
- Constrúyalas utilizando al menos 8 caracteres.

- Use claves distintas para equipos diferentes y/o sistemas diferentes.
- Use un acrónimo de algo fácil de recordar Ej: NorCarTren (Norma , Carlos, Tren)
- Añada un número al acrónimo para mayor seguridad: NorCarTren09 (Norma, Carlos, Tren, Edad del hijo)
- Mejor aún, si la frase origen no es conocida por otros: Verano del 42*:* Verdel4ydos
- Elija una palabra sin sentido, aunque pronunciable. (galpo-glio)
- Realice reemplazos de letras por signos o números. (3duard0palmit0)
- Elija una clave que no pueda olvidar, para evitar escribirla en alguna parte. (arGentina5-0)
- Cuide que no lo vean cuando digita su clave.
- Absténgase de observar a otros mientras lo hacen.
- Evite escribir la clave en papelitos, ni post-it, ni en archivos sin cifrar.
- Evite compartir su clave con otros.
- Absténgase de habilitar la opción de “recordar claves” en los programas que utilice.
- Si por algún motivo tuvo que escribir la clave, evite dejarla al alcance de terceros (debajo del teclado, en un cajón del escritorio) y menos pegada al monitor.
- Evite enviar su clave por correo electrónico ni la mencione en una conversación, ni se la entregue a nadie, aunque sea o diga ser el administrador del sistema.
- Cambie regularmente su contraseña.

NOTA:
Absténgase de dar sus contraseñas o PIN por correo electrónico o por teléfono, ni los introduzca en páginas web a las que haya llegado siguiendo un link recibido en un correo. Su banco jamás se las pedirá de esta forma.

Firma electrónica

Los certificados electrónicos permiten realizar numerosos trámites con las Administraciones a través de Internet así como firmar los documentos electrónicos de forma que estos pueden sustituir al papel en documentos auténticos. Hay certificados para personas físicas, como el DNI electrónico, y para empresas, como los emitidos por las Cámaras de Comercio (Camerfirma), los Registradores (SCR) o los Notarios (ANCERT).
Otra clase de certificados son los de servidor. Estos no se utilizan para firmar, sino que identifican a los sitios web y cifran la conexión para que no pueda ser leída por terceros. Evite introducir o solicitar datos en Internet sin que la conexión esté cifrada.

NOTA:
Desde 2002 las facturas con firma electrónica tienen plena validez legal. Piense en los árboles y el dinero que se ahorrarían enviando por correo electrónico al menos parte de las facturas que hoy se envían en papel.

Política de escritorio limpio

sitio.mv-tel.com

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todo el personal de la EAM debe evitar dejar activos de información, que se clasifiquen como restringidos o confidenciales, en los puestos de trabajo al alcance de otras personas en los momentos de ausencia. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

Control de acceso físico

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro; tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

Los equipos que hacen parte de la infraestructura tecnológica de la EAM tales como; servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios

que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

VENTAJAS DE APLICAR LA GUÍA PARA LA SEGURIDAD DE LA INFORMACIÓN.

- Reducción de riesgos debido al establecimiento y seguimiento de controles sobre ellos.
- Reducción de amenazas hasta alcanzar un nivel asumible por la institución.
- Si se produce una incidencia, los daños se minimizan y la continuidad de la institución está asegurada.
- Ahorro de gastos derivados de una racionalización de los recursos, eliminando las inversiones innecesarias e ineficientes; como las producidas por desestimar o sobrestimar los riesgos.
- La seguridad de la información deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado en el que participa toda la institución.
- La institución se asegura del cumplimiento de la legislación vigente y se evita riesgos y costos innecesarios.
- La institución se asegura del marco legal que protege a la empresa de aspectos que probablemente no se habían tenido en cuenta anteriormente.
- Contribuye a mejorar la competitividad en el mercado, diferenciándola de las demás instituciones, haciéndola más fiable e incrementando su prestigio.
- Mejora la imagen y confianza de la institución entre clientes y proveedores.

BIBLIOGRAFÍA

- ARCET. Fundamentos de la seguridad de la información. Consultado en: www.acert.gov.ar

- Archivo General de la Nación. Acuerdo 047 (05 de mayo de 2000).
- Archivo General de la Nación. Acuerdo No. 056 (05 de julio de 2000). Consultado en: www.archivogeneraldelanacion.gov.co

- Congreso de la República. Ley 1273 (05 de enero de 2009). Consultado en: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

- Espinosa Ramírez, Liliana; Ferreira, Nilson. (2013). Módulo de Herramientas Telemáticas. Universidad Nacional Abierta y a Distancia. Programa de Ingeniería de Sistemas

- Formación Activa. Manual para la gestión documental 2014. Págs. 344 – 351

- Gobierno de Aragón. Departamento de ciencia, tecnología y universidad. Guía para la seguridad de la información en su empresa. Consultado en: http://www.aragon.es/estaticos/GobiernoAragon/Departamentos/CienciaTecnologiaUniversidad/Areas/03_Sociedad_Informacion/Textos/si1.pdf

- Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior. Política General de Seguridad de la Información. Consultado en: www.icetex.gov.co

- Norma Técnica Ntc-Iso/Iec Colombiana 27001 Consultado en: http://www.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

- Universidad Tecnológica de Pereira. Políticas de Seguridad de Activos de Información. Consultado en: http://media.utp.edu.co/sistema-de-gestion-de-seguridad-de-la-informacion/archivos/politicas_sgsi.pdf

Artículo Segundo. La presente Resolución rige a partir de la fecha de su aprobación y sustituye la Resolución Rectoral No. 090 del 24 de julio de 2014.

PUBLÍQUESE Y CÚMPLASE

Armenia, 12 de octubre de 2018.

FRANCISCO JAIRO RAMIREZ CONCHA
Rector

WILLIAM H. MARTINEZ MORALES
Secretario General