Política

SEGURIDAD EN TECNOLOGÍAS DE LA INFORMACIÓN

HISTORIAL DE REVISIONES

Fecha de revisión	Versión	Descripción	Autor	Revisado por	Aprobado por	Entrada en vigencia
29/XII/2016	1.1.0	Versión inicial.	Estela Beiroa / Andrea Antúnez / Diego Di Pascua	Diego Di Pascua / Martín Davidovich / Gabriela Blanco / Silvia Rossel / Daniel Rafaniello / Rosario García / Diego Lemus / Rosario Minerva / Miguel Sánchez	Directorio - RD Acta 191 24/V/2017	24/XI/2017

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Contenido

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

1. Alcance

La Política de seguridad en tecnologías de la información se expresa como “deber ser” y se toma como marco de referencia para todas las áreas.

Es de aplicación en todo el ámbito de la Institución. Atañe a todos los empleados, miembros del Directorio, miembros de la Comisión Asesora y de Contralor, consultores, personal contratado, proveedores de servicios y cualquier otra persona física o jurídica que tenga cualquier tipo de relación con la CJPPU.

Todas las personas alcanzadas por esta política deben estar en conocimiento de la misma, cumplirla y velar por su cumplimiento, cuidando en forma prioritaria la integridad, disponibilidad y confidencialidad de los activos de información de la CJPPU.

Siempre que sea posible y pertinente, la política debe estar contemplada en los contratos que la CJPPU establezca con terceros.

2. Revisiones

La Política de seguridad en tecnologías de la información será revisada con una periodicidad no mayor a tres años o en oportunidad de ocurrencia de eventos significativos, con el objetivo de incorporar los cambios derivados de los avances tecnológicos o metodológicos, así como las modificaciones en la estructura organizativa de la CJPPU o en regulaciones y normas internas o externas.

3. Antecedentes

La Caja de Jubilaciones y Pensiones de Profesionales Universitarios (CJPPU) tiene una **Política General de Seguridad de la Información**, aprobada por RD 14/10/1998, en cuyo marco se incorpora la presente Política de Seguridad en Tecnologías de la Información.

Además, la CJPPU tiene políticas aprobadas en RD 09/08/2006 y RD 23/08/2006, donde se definen los propietarios de sistemas, programas y datos de la Institución y sus usuarios, así como las potestades y responsabilidades de propietarios, usuarios, División Informática y Auditoría Interna.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Dichas políticas son:

- **Política de roles en el desarrollo y mantenimiento de sistemas informáticos, programas y datos**
- **Política de roles en el control de acceso a sistemas, programas y datos**

3.1 Política General de Seguridad de la Información

A continuación, se transcribe la Política General de Seguridad de la Información, aprobada en RD 14/10/1998.

Política de Seguridad de la Información

I Definición y alcance de la política

Es de alta prioridad para la Organización:

1 Asegurar que los importantes activos de información que se procesan en forma manual o automatizada preserven en todo momento las siguientes tres cualidades básicas:

a Integridad. Es la condición de que la información se mantenga en todo momento al amparo de situaciones que puedan destruirla, modificarla sin la debida autorización, o afectar su confiabilidad y exactitud.

b Disponibilidad. Es la condición de que la información pueda estar inmediatamente accesible cuando sea requerida por razones funcionales.

c Confidencialidad. Es la condición de que la información se maneje con el debido cuidado ante situaciones de distinta índole que puedan directa o indirectamente dañar los intereses de la Institución o a alguno de sus asociados.

2 Velar por el cumplimiento de las disposiciones legales, reglamentarias y contractuales vinculadas al área de sistemas de información.

3 Contar con un plan de continuidad de los sistemas de información, que deberá ser mantenido permanentemente y probado periódicamente.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

4 Brindar capacitación y entrenamiento al personal, ajustados a los requerimientos de los distintos niveles (gerencial, mandos medios, personal en general) y que se traduzca en un plan de educación continua que asegure un adecuado nivel de concientización y formación que contribuya a los fines de la presente política.

5 Asegurar que la auditoría interna realice un permanente seguimiento de las operaciones de los sistemas a fin de garantizar su confiabilidad.

6 Aplicar la universalmente reconocida y aceptada normativa propietario-usuario-proveedor del servicio, en base a los siguientes criterios:

a Las gerencias de línea, con excepción de la División Informática, deberán cumplir el rol de propietarios o usuarios de procesos y datos.

Serán propietarios y responsables del correcto funcionamiento lógico de los procesos informáticos que se ejecuten en el ámbito de sus respectivas gerencias y propietarios de los datos que por razones de competencia sean originados y actualizados en el marco de su jurisdicción.

Serán usuarios de los procesos y los datos, cuando por razones funcionales se requiera el acceso a la ejecución de los procesos o la visualización de los datos con la previa autorización del propietario de los mismos.

b La División Informática habrá de cumplir el rol de proveedor del servicio y custodio de los equipos que almacenan los procesos y datos de toda la Organización.

II Responsabilidades de los roles establecidos

1 Propietario de los procesos

Es responsabilidad del propietario de los procesos:

- *Especificar los requerimientos de los procesos informáticos 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.*
- *Asegurar que los usuarios sean adecuadamente entrenados en el uso del sistema.*
- *Autorizar a usuarios a desarrollar funciones a través de procesos de su propiedad.*
- *Especificar los controles que el proceso requiere.*

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

- *Determinar los requerimientos de continuidad de la función que su repartición cumple.*

2 *Propietario de los datos*

Es responsabilidad del propietario de los datos:

- *Determinar las necesidades en materia de datos para el cumplimiento de su función.*
- *Tomar todas las medidas que estén a su alcance, para asegurar la debida integridad, disponibilidad y confidencialidad de los datos.*

3 *Usuario de procesos y datos*

Es responsabilidad del usuario de procesos y datos:

- *Proteger el equipamiento para procesamiento de datos que se encuentra bajo su custodia.*
- *Mantener los controles apropiados sobre sus tres áreas de contacto con el sistema a procesar:*
  - *el acceso al mismo*
  - *la entrada de datos*
  - *los informes producidos*
- *Cumplir con los requerimientos de seguridad de la información vigentes en la Institución.*

4 *Proveedor del servicio*

Es responsabilidad del proveedor del servicio:

- *Asegurar que en caso de falla, todos los procesos puedan ser restaurados a la brevedad, con un mínimo de sacrificio para la Institución y de acuerdo al plan de contingencias y de recuperación de desastres.*
- *Asegurar que los servidores de datos o procesos tengan la capacidad suficiente para proveer un adecuado nivel de servicio para toda la Organización.*
- *Conducir la puesta en marcha de un programa de seguridad de la información en nuestra Organización que supone la implantación y la permanente actualización y seguimiento de las medidas preventivas, detectivas y correctivas que permitan mantener en todo momento un adecuado nivel de seguridad, sin perjuicio del control independiente que habrá de llevar adelante la Auditoría Interna.*

III Implantación de la política

Las gerencias llevarán adelante la implantación de la Política de Seguridad de la Información, ejerciendo el rol de propietario, usuario o proveedor del servicio y asegurando que el personal a su cargo interprete y ejecute adecuadamente las tareas encomendadas.

La puesta en marcha de esta política será antecedida por la capacitación y entrenamiento de todo el personal involucrado.

4. Clasificación de la información

Para el cumplimiento de su cometido, que consiste en brindar coberturas en las contingencias de seguridad social determinadas en su Ley Orgánica, que ocurran a los integrantes del colectivo que incluye (art. 2° Ley 17.738), la CJPPU dispone de un cúmulo de **datos personales**, entendiendo por tales todos aquellos que impliquen información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, según los términos del art. 4° Ley 18.331.

Ello implica que, en su carácter de entidad pública alcanzada por esa normativa, tiene el deber de efectuar un tratamiento de esos datos acorde con ésta.

Así, destacan entre las disposiciones relevantes con relación a la temática de política de seguridad en tecnologías de la información –sin que la enumeración tenga carácter excluyente–, los contenidos de los artículos 4° (definiciones), 5° a 12° (principios generales), 13° a 17° (derechos de los titulares de los datos), 18° y 19° (datos especialmente protegidos) de la premencionada ley.

Por otra parte, la Caja posee, en atención a su naturaleza paratributaria, información de carácter **confidencial** y eventualmente la que pueda clasificarse como **reservada**, cuya regulación está contenida en la Ley 18.381, de la que destacan al respecto sus artículos 9° a 11°.

5. Protección de la información

Como principio de seguridad de la información, cualquiera sea la forma que tome la misma o los medios por los que se transmita, comparta o almacene, debe estar siempre adecuadamente protegida.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

En particular, la información confidencial o reservada:

- debe ser protegida contra la divulgación no autorizada a través cualquier medio físico o electrónico
- si fuera transportada o transmitida por fuera de los sistemas y redes institucionales (Internet, cartuchos, discos, pen-drives, etc.) deberá contar con protecciones especiales (cifrado, contratos, precintos, etc.)
- debe ser explícitamente identificada como tal y debe ser destruida al final de su vida útil (considerando los plazos precaucionales definidos por la CJPPU)
- en caso de ser necesario imprimirse, debe hacerse de acuerdo a un procedimiento que se ajuste a la normativa vigente

En caso de ser necesario y posible enviar información confidencial o reservada a organismos o personas externas, la entrega debe realizarse con un marco legal o acuerdo específico entre partes que garantice que la información será utilizada solamente para los fines acordados y que su seguridad será garantizada por el destinatario, en relación a todos los aspectos contemplados por la Política General de Seguridad de la Información y por la Política de Seguridad en Tecnologías de la Información de la CJPPU.

6. Seguridad lógica

6.1 Uso de sistemas

6.1.1 Controles de acceso

Debe controlarse el acceso a los sistemas de información a través de identificadores únicos, los que no habrán de ser compartidos.

Los usuarios serán personales e intransferibles, con excepción de los usuarios genéricos que se necesiten para para ejecutar tareas específicas. En este último caso, se deberá documentar la excepción y se mantendrá la responsabilidad funcional de los involucrados sobre dichas tareas.

La administración de los usuarios predefinidos en el software adquirido a terceros debe ser realizada como si fueran usuarios reales, siempre que sea técnicamente posible.

El acceso a las contraseñas de los usuarios genéricos o predefinidos estará fuertemente restringido sobre la base de los principios "necesidad de saber" y "necesidad de hacer".

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Toda solicitud de alta, baja o modificación de usuarios o privilegios de acceso a sistemas y servicios informáticos debe estar debidamente autorizada, y se debe registrar tomando las medidas necesarias para garantizar la confidencialidad, integridad y disponibilidad de dicha información.

Debe existir un proceso formal, en relación a los sistemas de información, para la administración de las solicitudes de alta, baja y modificación de usuarios, así como de cambio de identificador.

Los privilegios de acceso de los usuarios, sistemas y programas, deben estar restringidos sobre la base de los principios: “necesidad de hacer”, “necesidad de saber”, “separación de funciones” y “oposición de intereses”.

6.1.2 Autenticación de los usuarios

Los usuarios deben identificarse y autenticarse mediante identificadores únicos (usuario y contraseña o medios criptográficos), al inicio de cada sesión a los sistemas.

Las contraseñas de los usuarios deben estar sujetas a reglas definidas por la División Informática, con el fin de minimizar los riesgos de violación de la seguridad lógica.

Dichas reglas deben establecer, al menos, que:

- el sistema de acceso deba obligar a los usuarios a cambiar la contraseña una vez transcurrido el período de cambio obligatorio
- el sistema de acceso deba obligar a los usuarios a cambiar la contraseña la primera vez que el usuario ingresa al sistema después del alta o de un cambio de contraseña
- las contraseñas no puedan reutilizarse antes de una cantidad definida de cambios de contraseña
- las contraseñas tengan un largo y complejidad suficiente para desestimular ataques de deducción, de diccionario o de fuerza bruta

Los medios criptográficos que se utilicen para identificar a los usuarios deben utilizar algoritmos y claves que se consideren de alta calidad de seguridad en el momento de su utilización.

Las contraseñas o claves de acceso deben memorizarse, estando prohibido escribirlas (en papel, en correos electrónicos, en documentos, en notas, etc.), imprimirlas o almacenarlas digitalmente. La única excepción a esto último refiere a las contraseñas de administración que deben guardarse cifradas para una eventual recuperación en caso de faltar los técnicos. La clave de descifrado debe estar en

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

conocimiento del Jefe del Departamento de Producción y Soporte Técnico, el Gerente de Informática y el Gerente General.

Debe evitarse marcar la opción de “recordar contraseña” en cualquier aplicativo, para reducir el riesgo de accesos de otra persona y porque habitualmente los aplicativos almacenan las contraseñas en forma poco segura.

Varios sistemas y aplicativos de la CJPPU guardan registros de auditoría referidos a accesos y datos visualizados y modificados. La persona será responsable de las operaciones que se realicen con su usuario.

6.1.3 Controles para accesos remotos

Cuando se deba acceder a algún recurso desde fuera de las redes de la CJPPU, se deberán utilizar los mecanismos de seguridad definidos, y deberá existir un procedimiento para las solicitudes de alta, baja y modificación de estas autorizaciones.

6.1.4 Revocación de derechos de acceso

Deben revisarse los derechos individuales de acceso cuando se alteran las tareas de un usuario.

Se debe bloquear el acceso para un usuario si no es utilizado por un período determinado.

Los derechos de acceso a la información y los medios de procesamiento de información de todos los usuarios alcanzados por la presente política deben ser retirados a la terminación del vínculo con la CJPPU que hacían necesarios dichos derechos.

En el caso de las casillas de correo electrónico de usuarios con derechos revocados, se generará una respuesta automática a cualquier correo que tenga ese destino, por al menos seis meses a partir de la revocación, para indicar que cualquier tema laboral debe ser remitido a la institución por otra vía o dirigido a otra casilla.

6.1.5 Controles de seguridad

Las sesiones de estaciones de trabajo sin actividad luego de un período determinado deben desconectarse automáticamente o bloquearse, en caso de ser posible.

Deben generarse rastros de auditoria para los usuarios con privilegios especiales (por ejemplo, usuario administrador de la base de datos), que permitan ser revisados

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

en forma independiente, adoptándose medidas para garantizar la confidencialidad, integridad y disponibilidad de dichos registros por un período mínimo de tres años.

Salvo por razones debidamente justificadas y documentadas, la cantidad de usuarios con permisos de administración sobre los sistemas de control de acceso debe estar restringida al mínimo indispensable para realizar eficientemente las tareas del cargo, debiendo existir “oposición de intereses” y “separación de funciones” entre los administradores de los sistemas de control de accesos (usuarios y permisos) y los administradores de recursos.

Los administradores de División Informática no deben acceder a los equipos de los usuarios sin el consentimiento de los mismos, incluyendo la asistencia remota, salvo por incidentes de seguridad y riesgos en la disponibilidad de los servicios informáticos. Cuando se haga uso de esta excepción, deberá comunicarse el hecho y su justificación al usuario o al superior inmediato del mismo, en forma inmediata y por un medio de comunicación fehaciente.

Ante una investigación administrativa, no se podrá acceder a la información sin un debido proceso que asegure la objetividad, autenticidad, conservación e inalterabilidad de la misma, debiendo documentarse lo actuado mediante acta notarial, y previa autorización de la línea jerárquica con un nivel no inferior a Gerente de División, y, cuando sea posible, el contralor de la persona involucrada o un representante por él designado.

6.2 Instalación y mantenimiento de software de base

La instalación y mantenimiento de versiones de software de base está a cargo de División Informática. Siempre que sea técnicamente posible se mantendrán actualizadas las versiones de sistemas operativos y software de base.

Cuando se trate de software propietario, todo software debe ser adquirido con licencia, la cual se renovará periódicamente mientras dicho software se encuentre en uso.

6.3 Controles sobre software malicioso

La CJPPU contará con software antivirus y antispam, cuya selección e implementación está a cargo de División Informática.

Los usuarios no deben intentar erradicar del equipo software malicioso: virus, troyanos, gusanos, spyware, etc. En caso de sospecharse una infección se debe dejar de utilizar el equipo y llamar al Departamento de Producción y Soporte Técnico en forma inmediata. Además, debe suspenderse el uso de cualquier dispositivo de almacenamiento utilizado en la computadora infectada.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Todo software, antes de su instalación o ejecución, debe ser revisado con el software antivirus a efectos de verificar que se encuentra libre de infección. Si el software está cifrado o comprimido deben verificarse, además, los archivos resultantes de su descifrado o descompresión.

Los archivos provenientes de una fuente externa solo pueden ser utilizados después de haber sido controlados con el software antivirus.

Todos los equipos informáticos deben tener instalado y funcionando en las condiciones establecidas el software antivirus seleccionado como estándar. Se prohíbe al usuario deshabilitarlo y realizar cambios en la configuración, los cuales pueden ser efectuados exclusivamente por el Departamento de Producción y Soporte Técnico.

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.

Deben instalarse en todos los equipos informáticos, todas las actualizaciones que el proveedor del software antivirus publique y que mejoren las capacidades del producto.

La División Informática enviará a todos los usuarios, cuando corresponda, información y material de referencia sobre los virus y los productos antivirus así como sobre las obligaciones y políticas establecidas.

6.4 Administración de sistemas

El administrador de sistemas, que requiera usuarios con permisos especiales sobre la información almacenada y transmitida, no puede leer, copiar, borrar, retener, desviar, divulgar o alterar información cuyo propietario o destino sea otro usuario.

Las únicas excepciones a esto son:

- copias para respaldar la información
- si hay un pedido expreso y por escrito del usuario propietario o destino de la información, validado por su gerente de división o el Gerente General

6.5 Pruebas de seguridad

Está prohibido realizar pruebas de controles, pruebas de vulnerabilidad o pruebas de penetración, así como la instalación o uso de herramientas informáticas que permitan alterar, burlar o desactivar los sistemas de la infraestructura de red, a excepción de los trabajos de control habituales de los administradores de sistemas de

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

la CJPPU o los servicios expertos de “hackeo ético” debidamente autorizados mediante contrato.

7. Seguridad física

7.1 Servidores e infraestructura de red

Los servidores, UPS y dispositivos de red centrales deben estar alojados dentro de una sala de servidores. La División Informática definirá para cada equipo si se instala en la sala de servidores central o en la de contingencia.

Se debe contratar servicio de mantenimiento de hardware siempre que esto mejore la seguridad de la información.

El acceso físico a los dispositivos de red distribuidos debe estar protegido ante personas no autorizadas.

7.2 Soporte de almacenamiento de respaldos

Debe disponerse de un servicio externo para el transporte, almacenamiento y custodia de respaldos de información computarizada en bóvedas de seguridad situadas fuera de la CJPPU.

Los soportes de almacenamiento de respaldos (por ejemplo, cintas) deben almacenarse, en todo momento, en forma protegida frente al acceso de personas no autorizadas.

Los soportes de almacenamiento de respaldos que preserven el histórico de la información (por ejemplo, cintas de fin de mes) se deben almacenar en un mueble especial, ignífugo y con cerradura, destinado a tales efectos.

7.3 Sala de almacenamiento de suministros

La sala de almacenamiento de suministros debe permanecer, en todo momento, protegida de acceso de personas no autorizadas.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

7.4 Control de acceso físico

El control de acceso físico está diseñado para proteger a la organización contra los accesos no autorizados al hardware que contenga o transmita la información del organismo.

El acceso a la sala de servidores central y de contingencia, así como el acceso a los tableros eléctricos que comandan la alimentación de los equipos informáticos contenidos en ellas, está restringido al personal autorizado a tales efectos, de acuerdo a los procedimientos establecidos.

Para el acceso a cualquiera de las salas de servidores se utilizarán controles de autenticación que validen y autoricen todos los accesos, manteniendo registros de auditoría con la identificación, fecha y hora relativa a toda entrada o salida de los mismos. Se adoptarán medidas para garantizar la confidencialidad, integridad y disponibilidad de dichos registros por un período mínimo de seis meses.

El acceso de personal de servicio de apoyo de terceros a las áreas controladas solo se realizará cuando sea estrictamente necesario. Este acceso deberá ser autorizado y monitoreado por personal de División Informática que tenga permisos para ello.

7.5 Desecho, reutilización o envío a reparación de equipamiento informático

Antes de desechar, reutilizar o enviar a reparación externa a cualquier equipamiento informático, se deberán verificar los medios de almacenamiento contenidos, para asegurarse que se haya retirado o sobreescrito (de modo que sea imposible recuperar la información original), cualquier licencia de software o información confidencial o reservada.

7.6 Control Ambiental

Las salas de servidores de la CJPPU deben contar con dispositivos para la detección y monitoreo de temperatura, humedad e incendio. También, con fuentes de energía ininterrumpible (UPS, bancos de batería y generadores si corresponde) para garantizar los niveles de disponibilidad acordados con los propietarios de la información, sistemas y programas contenidos los servidores de cada sala.

Deben tomarse los recaudos necesarios para asegurar un ambiente con los niveles de temperatura y humedad requeridos por los fabricantes del equipamiento informático.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Las salas de servidores no deben contar con elementos inflamables dentro del recinto.

Las ventanas de vidrio deben estar protegidas de forma de evitar el estallido ante el calentamiento por fuego o rotura.

7.7 Instalación y mantenimiento de hardware y redes

Todo dispositivo conectado a la red interna debe ser instalado por el Departamento de Producción y Soporte Técnico, y el software de base debe ser provisto por la CJPPU.

Cuando se trate de un software provisto por terceros, quien lo proporcione debe proveer a la CJPPU del software específico y su manual de instalación. La instalación se realizará por personal interno idóneo, con asistencia del proveedor cuando se entienda necesario.

7.8 Uso de infraestructura

7.8.1 Puestos de trabajo e impresoras

Cada usuario tendrá asignado un puesto de trabajo (computadora de escritorio o laptop) de uso personal para fines exclusivamente laborales, que eventualmente se podrá compartir dentro del departamento o sector.

Las impresoras serán utilizadas con fines exclusivamente laborales y se asignarán por área, distribuyéndose en acuerdo entre la División Informática y las gerencias respectivas.

7.8.2 Dispositivos móviles

A los efectos de la presente política se consideran dispositivos móviles los teléfonos celulares inteligentes, tabletas, lectores tipo PDA y computadores portátiles (laptops, netbooks).

El responsable de autorizar el uso de dispositivos móviles de CJPPU a los usuarios debe ser un superior de nivel gerencial.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

7.8.2.1 Condiciones de uso

Los dispositivos móviles provistos por la CJPPU deben utilizarse para actividades de carácter laboral, pudiendo usarse para otros fines solamente si esto no afecta la seguridad de la información de la organización ni la integridad de la instalación.

De los mismos, solamente las computadoras portátiles (tipo laptop) que sean usadas exclusivamente como estaciones de trabajo del organismo pueden almacenar información confidencial o reservada de la CJPPU y conectarse a la red interna en condiciones similares a las estaciones de trabajo fijas. Los dispositivos que sean utilizados con fines multipropósito (teléfonos celulares, tablets, computadoras portátiles destinadas a eventos o presentaciones varias, etc.) no pueden almacenar información confidencial o reservada de la CJPPU ni conectarse a la red interna donde se transmita información confidencial o reservada de la CJPPU.

Los usuarios no tienen permitido realizar ni autorizar ningún arreglo o servicio para el dispositivo que tenga asignado, debiendo canalizar los pedidos correspondientes a través del Departamento de Compras y Servicios Generales.

7.8.2.2 Pérdida o robo de dispositivos de la CJPPU

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 de la situación al Departamento de Compras y Servicios Generales y a su gerente de División o Secretaría de Directorio, así como realizar la denuncia policial correspondiente. Esta notificación y la denuncia deben tener lugar para poder cancelar cualquier servicio móvil asociado al dispositivo, así como también intentar borrar remotamente la información contenida en la memoria del mismo. El usuario debe configurar su dispositivo, siempre que sea posible, para permitir este extremo.

7.8.2.3 Funcionalidades y características de manejo

En cuanto a las computadoras portátiles que se utilicen como estaciones de trabajo, el hardware, sistema operativo y utilitarios que se encuentren instalados en el momento de la entrega del equipo al usuario no deben sufrir cambios a menos que hayan sido requeridos o autorizados por el Departamento de Producción y Soporte Técnico.

En todos los casos, no está permitido que el usuario realice el desbloqueo de las limitaciones del fabricante o proveedor (root, jailbreak, etc.), o que realice cualquier otro método de cambio de las protecciones.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

7.8.2.4 Obligaciones de seguridad para los datos

Los usuarios deben tomar las apropiadas precauciones para prevenir que personas externas a la organización tengan acceso a los dispositivos móviles de la CJPU y los recursos asociados a los mismos.

Los usuarios no deben:

- compartir el dispositivo
- compartir usuario, contraseña, PIN u otro tipo de credencial

7.8.2.5 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 CJPPU.

Las instalaciones no gestionadas o no aprobadas comprometen el ambiente operativo y también constituyen un riesgo de seguridad, incluyendo (con o sin intención): comprometer información confidencial o reservada, esparcir software malicioso, permitir accesos no autorizados, etc.

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 ser dejados en un vehículo desatendido
- los dispositivos deben estar posicionados de manera que no queden visibles desde una ventana accesible desde el exterior
- si en la pantalla de un dispositivo móvil se está mostrando información confidencial o reservada, se debe posicionar de tal manera que la información no pueda ser vista por personas no autorizadas
- en situaciones vulnerables (aeropuertos, hoteles, centros de conferencias, etc.), el dispositivo no debe quedar desatendido bajo ninguna circunstancia
- los dispositivos deben ser cargados como equipaje de mano cuando se viaja
- el dispositivo habilitado para ello debe mantener solamente la información de la CJPPU que sea imprescindible para fines laborales

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

7.8.3 Correo electrónico y mensajería instantánea

El correo electrónico y la mensajería instantánea son herramientas de trabajo suministradas por la CJPPU, y el permiso de acceso a los mismos se otorgará mediante los procedimientos establecidos de alta, baja y modificaciones de permisos a usuarios.

Existen varios tipos de casillas:

- casillas de correo individuales, siendo que cada empleado o autoridad tiene la propia
- casillas de correo institucionales, donde la dirección de correo electrónico es asociada a una función específica, evento, congreso, etc.
- casillas compartidas, donde varios usuarios (cada uno usando su propia cuenta) tienen permisos de utilización de la casilla

Además, pueden definirse listas de distribución, siendo que los correos que lleguen a una lista se distribuirán entre las casillas que la compongan.

Toda casilla de correo electrónico individual será de uso personal, intransferible y exclusivamente con fines laborales. Por excepción se permite ocasionalmente el uso particular, siempre y cuando el consumo de recursos o el contenido no comprometan la seguridad de los sistemas de información ni la imagen de la organización.

Por su parte, las casillas institucionales no estarán asociadas a una persona en particular. Por ende, los correos electrónicos recibidos podrán ser automáticamente dirigidos a un grupo de personas que la CJPPU estime conveniente para el desarrollo de dicho propósito o función laboral.

El emisor de un correo electrónico debe incluir al menos, al pie del correo, los datos que identifiquen la institución (logo, dirección, sitio web), los datos que identifiquen la persona que envía el correo (nombre, apellido, cargo, departamento al que pertenece, teléfono de contacto), un aviso de confidencialidad y privacidad referido al contenido del correo y un exhorto a no imprimir el correo. Dicho pie tendrá un mismo formato y contenido para toda la organización.

Está prohibido el uso del correo electrónico para enviar mensajes de tipo “cadena”.

Para la difusión de información corporativa, será necesaria una autorización escrita con nivel gerencial.

Cada casilla tendrá asignado un determinado espacio de acuerdo a los procedimientos que se establezcan a tal fin.

La CJPPU podrá rechazar conexiones de correo electrónico desde direcciones de correo electrónico o servidores externos cuando haya razones de seguridad que lo ameriten.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

No se deben ejecutar programas que integren o que lleguen adjuntos en correos o mensajes de una fuente no reconocida, ya que los mismos pueden contener virus que afecten a los recursos de la institución.

El acceso a través de Internet al correo electrónico (utilizando cualquier dispositivo) será autorizado de acuerdo a los procedimientos que se establezcan a tal fin.

La información confidencial o reservada contenida en un correo electrónico solamente podrá ser transmitida a servidores externos a la CJPPU si dicha información se cifra con algoritmos y claves que se consideren de alta calidad de seguridad en el momento de su utilización.

7.8.4 Servidor de archivos

El servidor de archivos es una herramienta de trabajo suministrada por la CJPPU y el permiso de acceso al mismo se otorgará mediante los procedimientos establecidos de alta, baja y modificaciones de permisos a usuarios.

Cada repartición (división, departamento, sector, etc.) tendrá asignado un determinado espacio en la red para el almacenamiento de archivos, de acuerdo a los procedimientos que se establezcan a tal fin.

Asimismo, cada usuario tendrá asignado un determinado espacio de acuerdo a los procedimientos que se establezcan a tal fin.

Solamente se podrá almacenar en el servidor de archivos información relacionada con la actividad laboral de la CJPPU y que sea de interés institucional que se respalde.

7.8.5 Internet

El acceso a Internet constituye una herramienta de trabajo suministrada por la CJPPU y el permiso correspondiente se otorgará mediante los procedimientos establecidos.

Ante indicios de amenazas a la seguridad de información o a la incorrecta utilización del servicio, División Informática controlará el acceso a Internet, y ante la comprobación de un problema dará aviso a la línea jerárquica correspondiente, pudiendo suspender los permisos de acceso que corresponda.

Toda la información que la CJPPU publica en páginas web en Internet debe ser revisada sistemáticamente por el área funcional dueña de la información, para verificar que no haya sido alterada.

Toda aplicación a ser utilizada en ambiente de Internet debe estar sujeta a pruebas de vulnerabilidad antes de ser puesta en producción.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

7.8.6 Escritorio limpio

Toda vez que un usuario se ausenta de su lugar de trabajo debe guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial o reservada.

Además, si se ausenta de forma temporal durante la jornada, debe bloquear su estación de trabajo de forma que para desbloquearla haga falta el ingreso de su contraseña u otra forma de autenticación segura. Por su parte, al finalizar la jornada de trabajo, debe desconectarse de los servidores y estaciones de trabajo de oficina.

La información confidencial o reservada que se imprima debe retirarse inmediatamente de las impresoras.

7.8.7 Infraestructura de red

Está prohibido conectar dispositivos que transmitan o reciban información en un puesto de red sin previa autorización de División Informática.

Está prohibido conectar dispositivos eléctricos en los tomacorrientes que están dedicados a puestos de trabajo, impresoras y demás equipos informáticos sin previa autorización de División Informática.

8. Desarrollo de sistemas informáticos

La seguridad en aplicaciones es el uso de principios o buenas prácticas de seguridad aplicadas durante el ciclo de vida del software.

La política de seguridad de las aplicaciones implica implementar los requisitos de seguridad establecidos; es decir, la aplicación que se desarrolle debe adaptarse al modelo de seguridad definido.

La disponibilidad de los requisitos de seguridad hace posible que el equipo de desarrollo pueda crear y mantener un software con una mentalidad de privilegios mínimos, de tal forma que pueda implementarse garantizando la integridad, disponibilidad y confidencialidad de la información.

La Política parte de tener definidos los roles y responsabilidades en el proceso de desarrollo y mantenimiento de los sistemas y en la propiedad de los sistemas, programas y datos (RD 09.08.2006 y RD 23.08.2006, Res. N° 1066/2006).

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

En este capítulo, se detallan los requisitos y controles que se entienden necesarios para que la seguridad sea una parte integral del desarrollo y mantenimiento de los sistemas, y asegurar que los mismos:

- cumplen con los requerimientos de la Institución
- incluyen un nivel adecuado de seguridad y control
- son probados, documentados y cuentan con la aceptación de los usuarios propietarios antes de ser puestos en producción

La metodología de desarrollo debe incluir:

- especificación de requerimientos funcionales y de seguridad
- niveles de prueba
- procedimientos de implementación
- pruebas de aceptación por los responsables funcionales
- control de versiones

Todo software desarrollado en la CJPPU por personal propio o ajeno es propiedad intelectual de la CJPPU.

El acceso a modificar el código fuente de las aplicaciones y los ítems asociados (especificaciones, diseños, planes de verificación y validación) será restringido al personal de División Informática.

Se establecen requisitos y controles de seguridad para cada fase del Ciclo de Desarrollo.

Especificación

Toda solicitud de desarrollo o mantenimiento debe contar con una especificación formal y aprobada por el propietario.

En la especificación deben quedar justificados, acordados y documentados los requerimientos de seguridad.

Se deben definir los controles de autenticación, roles y privilegios de los usuarios del sistema a desarrollar o a realizar mantenimiento correctivo.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Diseño

Los requerimientos definidos y aprobados deben diseñarse con el objetivo de prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones.

El modelo de diseño debe estar orientado a la seguridad.

Se deberán validar los datos de ingreso en las aplicaciones para asegurar que estos datos sean correctos y apropiados.

Todos los accesos se controlarán.

Se incluirán controles para detectar los siguientes errores:

- valores fuera de rango
- caracteres inválidos en los campos de datos
- datos incompletos o faltantes
- datos de control de no autorizado o inconsistentes
- procedimientos o mensajes para avisar o responder a los errores de validación

El diseño debe asegurar minimizar los riesgos de fallas en el procesamiento interno que lleven a la pérdida de integridad de la información.

Se deberán validar los datos de salida para asegurar que el procesamiento de la información almacenada sea el correcto y apropiado.

La información de salida debe ser exacta, precisa y suficiente para el usuario o el sistema de procesamiento.

Se deberá diseñar la solución informática con el criterio de separación de funciones, para permitir la estandarización y reutilización de las funciones de seguridad.

En el diseño de aplicaciones web, se diseñará en base a las siguientes premisas:

- diseñar los controles criptográficos para la gestión de claves con el fin de proteger la confidencialidad, autenticidad e integridad
- contemplar la seguridad de las comunicaciones en servicios accesibles por redes públicas
- diseñar un manejo seguro de sesiones

Se incluirán registros de auditoría en todas las nuevas estructuras de datos relevantes, para registrar los usuarios que agreguen, modifiquen o borren información.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Programación

Se deberán implementar todos los requerimientos de seguridad especificados y diseñados.

Se contará con ambientes de desarrollo y prueba independientes del ambiente de producción.

Las solicitudes de programación deberán ser implementadas y modificadas de acuerdo a los documentos de especificación y diseño, siguiendo las siguientes buenas prácticas:

- validación de entradas
- validación de salidas
- utilización de estándar de programación definido
- manejo apropiado de errores

Pruebas

La fase de pruebas incluirá el control de calidad de los controles de seguridad definidos y aprobados.

Las pruebas deberán incluir:

- pruebas de caja negra, para asegurar que cada función es operativa, que la entrada que se acepta es la adecuada y que se produce una salida correcta
- pruebas de caja blanca, para asegurar que la operación interna se ajusta a las especificaciones, comprobando los caminos lógicos del programa
- pruebas de performance

Se requerirán pruebas de aceptación por parte de los propietarios y usuarios del sistema.

Puesta en producción

Se definirán procedimientos específicos para el pasaje de programas, módulos y sistemas desde el ambiente de desarrollo al ambiente de producción, a los efectos de que dichos pasajes se realicen con la debida autorización, y en forma controlada y coherente.

Los programas no deben ser modificables en ambiente de producción.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

9. Adquisición de hardware, software y servicios

Siempre que se requiera la adquisición de hardware, software o servicios para procesar información de la CJPPU se deberán evaluar los antecedentes del proveedor, la continuidad y certificaciones del proceso, producto o servicios.

La seguridad debe ser considerada desde la especificación de los requerimientos hasta su implementación y los requerimientos de seguridad deben estar identificados y documentados.

Todo proveedor debe garantizar que el software o hardware no contiene ningún código desarrollado que ponga en riesgo la seguridad informática de la CJPPU. En caso de detectarse tal tipo de código, el proveedor deberá emplear todos los esfuerzos razonables consistentes con las prácticas de desarrollo comunes en la industria para resolverlo tan pronto como sea posible.

Las contraseñas que provea el proveedor deberán ser cambiadas, en forma inmediata una vez terminada su instalación, por otras que cumplan con las reglas definidas en la presente política, excepto que exista una razón técnica que lo haga desaconsejable (lo cual se deberá documentar).

Las adquisiciones de equipamiento informático, dispositivos móviles o software de uso corporativo deben ser gestionadas o validadas por División Informática.

Todo software que se adquiera deberá contar con una licencia que permita la realización de copias con fines de respaldo.

Para el caso de la compra de hardware, se deben establecer plazos razonables para las garantías de los equipos, que los equipos sean originales de fábrica y que el modelo ofertado no está discontinuado salvo razones debidamente documentadas.

10. Control del inventario de hardware y software

Se deberá realizar periódicamente un control del inventario de hardware y software, relacionando lo que debe ser con lo que efectivamente está operativo.

Lo relevado debe conciliarse con lo mantenido por el Departamento de Compras y Servicios Generales y por el Departamento de Producción y Soporte Técnico.

De constatarse diferencias, las mismas se documentarán y se generarán las instancias de corrección, diagnóstico de las causas y, si se entiende necesario, generación de incidentes.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

11. Continuidad

La información, las instalaciones y componentes críticos de tecnología de la información deben contar con alternativas adecuadas que permitan asegurar la continuidad de las operaciones de la CJPPU y reducir al mínimo los daños causados por una contingencia.

Ante esta eventualidad, deben estar vigentes planes y procedimientos que permitan que la organización restablezca los servicios críticos del negocio en los tiempos y condiciones establecidos por sus propietarios.

11.1 Plan de continuidad

Deben existir procedimientos de recuperación de los sistemas de información en caso de contingencia, que incluyan los niveles de criticidad acordados y documentados.

La importancia y urgencia de recuperación para los servicios y aplicaciones de tecnología de la información estarán definidos en el Plan de Continuidad. Para su elaboración, deberán realizarse análisis de riesgos, análisis de impacto en el negocio (BIA) y documentar los objetivos de punto de recuperación (RPO) y los objetivos de tiempo de recuperación (RTO).

La elaboración, mantenimiento y pruebas periódicas de los planes y procedimientos de continuidad, serán responsabilidad de cada uno de los responsables funcionales de la información y sistemas de la CJPPU. La División Informática participará en dichas acciones.

La División Informática debe acordar con los proveedores de servicios críticos, los acuerdos de nivel de servicio (SLA) correspondientes que permitan garantizar el restablecimiento en ocasión de una caída del servicio.

Deben almacenarse copias del Plan de Continuidad en lugares físicamente independientes, con los niveles de seguridad y control adecuados.

11.2 Respaldos

Debe existir una política de respaldos definida por División Informática.

El Departamento de Producción y Soporte Técnico realizará respaldos solamente de la información contenida en los servidores de la CJPPU. Por lo tanto, la información que sea relevante para la CJPPU debe alojarse en uno de esos servidores.

Los soportes conteniendo los respaldos deben protegerse adecuadamente durante el transporte desde y hasta su lugar de almacenamiento externo.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Debe definirse la frecuencia con que se hacen copias de respaldo y el período de conservación de los mismos.

Debe definirse la destrucción segura de los soportes conteniendo los respaldos.

Ante cambios de gran impacto, debe estar previsto un procedimiento para retornar a la situación anterior.

La información almacenada debe ser probada periódicamente para asegurar que sea recuperable.

Debe garantizarse para la información de respaldos, como mínimo, la misma confidencialidad que para la de origen.

Los procedimientos de restauración se deben verificar y probar regularmente a los efectos de asegurar que sean efectivos y que puedan ser completados en las condiciones y los tiempos asignados en los procedimientos correspondientes.

La recuperación de un respaldo debe realizarse solamente ante:

- el pedido por escrito de un usuario con permiso de acceso a dicha información, siempre que no ponga en riesgo la seguridad e integridad referencial de los datos
- la necesidad de recuperarse ante un incidente que implique pérdida de información

La solución integral de respaldos debe asegurar la confiabilidad y calidad acordada con los propietarios de la información.

12. Gestión de incidentes

Un incidente de seguridad en TI es la violación o amenaza inminente a la violación de una política de seguridad de la información implícita o explícita. También es un incidente de seguridad un evento que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad).

Un usuario, ante cualquier sospecha o evidencia de violación de seguridad informática o incumplimiento de la presente política, debe reportarlo a su línea jerárquica y además a División Informática.

De ser posible, el reporte debe realizarse de forma inmediata y brindando la mayor cantidad de datos posibles. De esta manera, toda la información recibida por el equipo permitirá analizar el caso, dar un mejor diagnóstico de la situación y resolver el problema con mayor eficacia.

Es recomendable que al detectarse problemas no se altere la evidencia y se mantenga el sistema tal cual está en el momento en que se advierte la anomalía.

Ante un incidente de este tipo, la línea jerárquica y la División Informática deben tomar las medidas pertinentes para minimizar el impacto en la continuidad del negocio.

En cualquier caso, todo el ciclo de vida del incidente de seguridad deberá ser documentado como referencia futura y como justificación de las acciones que se hayan tomado en virtud del mismo.

13. Capacitación

Todo el personal de la CJPPU debe participar de las actividades de capacitación necesarias para proteger adecuadamente los recursos de informáticos de la institución.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Glosario

Para propósitos de este documento, se aplican los siguientes términos y definiciones.

Activo de información

Aquellos datos o información que tienen valor para una organización.
[Fuente: Certuy]

Acuerdo de nivel de servicio

Acuerdo escrito que define las responsabilidades específicas del proveedor de servicios y las expectativas del cliente.
[Fuente: CNSSI 4009]

Amenaza

Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.
[Fuente: ISO/IEC 13335-1:2004]

Análisis de riesgos

Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

Área controlada

Área o espacio para el que la organización confía en que las protecciones físicas y de procedimiento proporcionadas son suficientes para proteger la información o sistemas de información, según los requisitos establecidos.

Autenticación

Verificación de la identidad de un usuario, proceso o dispositivo, a menudo como requisito previo para permitir el acceso a los recursos en un sistema de información.
[Fuente: NIST SP 800-53; NIST SP 800-53A; NIST SP 800-27; FIPS 200; NIST SP 800-30]

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Autorización

Privilegios de acceso otorgados a un usuario, programa o proceso o el acto de otorgar esos privilegios.
[Fuente: CNSSI 4009]

CJPPU

Caja de Jubilaciones y Pensiones de Profesionales Universitarios.

Cifrado

Aplicación de un algoritmo específico a los datos a fin de alterar su apariencia y volverlos incomprensibles, para que sólo puedan ser accedidos por el destinatario.

Confiabilidad

Capacidad de un producto de realizar su función de la manera prevista.

Continuidad del negocio

Capacidad de la organización para continuar con la entrega de productos o servicios después de un incidente de interrupción, a niveles predefinidos como aceptables.
[Fuente: ISO 22300]

Contraseña

Cadena de caracteres protegida, que es utilizada para autenticar la identidad de un usuario de un sistema informático o autorizar el acceso a los recursos del sistema.
[Fuente: FIPS 181]

Control

Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Datos

Información, sin importar la forma, contenida o procesada por el equipamiento de sistemas de información, redes de comunicaciones, o medios de almacenamiento. Pueden presentarse en diferentes medios incluyendo: copias impresas, medios magnéticos, fichas, almacenamientos en línea, materiales físicos, etc.

Especificación

Objeto de evaluación que incluye artefactos basados en documentos (por ejemplo, políticas, procedimientos, planes, requisitos de seguridad del sistema, especificaciones funcionales y diseños arquitectónicos) asociados con un sistema de información.
[Fuente: NIST SP 800-53A]

Evento de seguridad de la información

Ocurrencia identificada del estado de un sistema, servicio o red indicando una posible falla en la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.
[Fuente: ISO/IEC TR 18044:2004]

Gusano

Programa auto-replicante, auto-propagante y autónomo que utiliza mecanismos de redes para propagarse.
[Fuente: CNSSI 4009]

Incidente

Violación o amenaza inminente de violación de la seguridad informática, políticas, políticas de uso aceptable o prácticas de seguridad estándar.
[Fuente: NIST SP 800-61]

Incidente de seguridad de la información

Evento o serie de eventos inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información.
[Fuente: ISO/IEC 27035]

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Lineamiento

Descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas.
[Fuente: ISO/IEC 13335-1:2004]

Medio de procesamiento de la información

Sistema, servicio o infraestructura de procesamiento de la información, o local físico que los aloja.

Mínimo privilegio

Principio que establece que una arquitectura de seguridad debe diseñarse de manera que a cada entidad se le concedan los mínimos recursos del sistema y autorizaciones que la entidad necesita para desempeñar su función.
[Fuente: CNSSI 4009]

Necesidad de saber

Método de aislamiento de recursos de información basado en la necesidad de un usuario de tener acceso a ese recurso con el fin de realizar su trabajo, pero no más. Los términos "necesidad de saber" y "mínimo privilegio" expresan la misma idea. La necesidad de saber se aplica generalmente a las personas, mientras que el mínimo privilegio se aplica generalmente a los procesos.

Nivel de criticidad

Refiere a las consecuencias del comportamiento incorrecto de un sistema. Cuanto más graves sean los efectos directos e indirectos esperados de un comportamiento incorrecto, mayor será el nivel de criticidad.

Pruebas de penetración

Metodología de prueba en la que los evaluadores, utilizando toda la documentación disponible (por ejemplo, diseño del sistema, código fuente, manuales) y trabajando bajo restricciones específicas, tratan de eludir las características de seguridad de un sistema de información.

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Plan de continuidad del negocio

Procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar un nivel predefinido de operación seguida de la interrupción del negocio.
[Fuente: ISO-22300]

Política

Intención y dirección general expresada formalmente por la gerencia o dirección.

Proceso

Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman entradas (especificaciones, recursos, información, servicios, salidas de otros procesos) en salidas (productos, resultados, informaciones, servicios y materiales).

Proceso crítico

Proceso que da soporte sustantivo a los servicios previamente identificados como esenciales, y cuya interrupción degrada significativamente la capacidad del sector de dar correctas respuestas a la comunidad.
[Fuente: Certuy]

Recursos

Todos los activos, personas, habilidades, información, tecnología (incluidas la planta física y los equipos), las instalaciones, y los suministros e información (ya sean electrónicos o no) que una organización tiene que tener disponibles para su uso, cuando sea necesario, con el fin de operar y cumplir con su objetivo.

Registro de auditoría

Registro cronológico de las actividades del sistema. Incluye registros de los accesos al sistema y las operaciones realizadas en un período dado.
[Fuente: CNSSI 4009]

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Respaldo

Copia de los archivos y programas hechos para facilitar la recuperación, si es necesario.
[Fuente: NIST SP 800-34; CNSSI 4009]

Riesgo

Combinación de la probabilidad de un evento y su ocurrencia.
[Fuente: ISO/IEC Guía 73:2002]

RPO (por su sigla en inglés, Recovery Point Objective)

Punto en el que la información utilizada por una actividad debe ser restaurada para permitir que la actividad opere en la reanudación.

RTO (por sus siglas en inglés, Recovery Time Objective)

Período de tiempo después de un incidente en el que el producto o servicio debe ser reanudado o la actividad debe reanudarse.

Seguridad física

Conjunto tangible de controles, destinados a cubrir las amenazas ocasionadas por el acceso físico a los medios donde se encuentran los activos de información, ocasionadas tanto por el hombre como por la naturaleza de dichos medios.

Seguridad lógica

Conjunto de controles basados en software, comúnmente en sistemas de información, que soportan los objetivos de la declaración de la política de seguridad.

Troyano

Programa de computadora que parece tener una función útil, pero también tiene una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces explotando autorizaciones legítimas de una entidad de sistema que invoca el programa.
[Fuente: CNSSI 4009]

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay

Virus

Programa de computadora que puede copiarse e infectar una computadora sin permiso o conocimiento del usuario. Un virus, por ejemplo, podría corromper o eliminar datos en una computadora, utilizar programas de correo electrónico para copiarse a otros equipos, o incluso borrar todo en un disco duro.
[Fuente: CNSSI 4009]

Vulnerabilidad

Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.
[Fuente: ISO/IEC 13335-1:2004].

Caja de Jubilaciones y Pensiones de Profesionales Universitarios - Andes 1521 - Tel.: 2902 8941 - C.P. 11.100 - Montevideo - Uruguay