JORNADAS FEDERALES DE CIBERSEGURIDAD

LIC. NANCY GARNICA

Asesora de formación y capacitación de la Dirección Nacional de Ciberseguridad de Jefatura de Gabinete de Ministros de la Nación

"DIRECTRICES PARA LA ELABORACIÓN DE POLÍTICAS DE PROTECCIÓN DE LOS ACTIVOS DIGITALES EN LAS INSTITUCIONES"

Santa Cruz Gobierno de la Provincia
UTN Facultad Regional Santa Cruz
UNPA UARG
Jefatura de Gabinete de Ministros Argentina
Dirección Nacional de Ciberseguridad
Datastar
NUTANIX

Directrices para la elaboración de políticas de protección de los activos digitales en las instituciones

Lic. Nancy Garnica

27 de mayo de 2022

Seguridad de la información

En la actualidad, la tecnología e Internet son herramientas indispensables para el funcionamiento de cualquier organización y deben utilizarse de forma adecuada para evitar riesgos en la gestión de la información.

Para ello debemos considerar a la información como un activo más, es decir, como otros bienes y servicios requeridos para cumplir con los objetivos de una organización.

Esta información puede presentarse en diversos formatos y soportes, como por ejemplo, estar escrita en papel o impresa, almacenada en archivos digitales o físicos, transmitida por correo o medios electrónicos, estar contenida en videos, fotos, audios, etc.

Seguridad de la información

Y sin importar el formato en el que esté, la información gestionada en nuestra organización debe estar protegida desde su creación, durante su ciclo de vida y hasta su destrucción, desuso o archivo definitivo.

Es indispensable pensar que -hoy en día- la información puede ser objeto de peligros, amenazas y usos indebidos e ilícitos. Por lo tanto, se deben extremar las medidas para preservar su confidencialidad, integridad y disponibilidad.

Y pensando en esa protección, la Dirección Nacional de Ciberseguridad elaboró una serie de requisitos mínimos para elevar los niveles de seguridad de la información de los organismos públicos.

Activos de información

Son los recursos que tiene una organización para operar de acuerdo a sus objetivos.

Incluyen el hardware, el software, los dispositivos de comunicación, los elementos de apoyo y la información y los datos que están en cualquier soporte y formato, entre otros.

Requisitos Mínimos de Seguridad de la Información
(Decisión Administrativa 641/2021)

Objetivos

- Establecer lineamientos generales y mínimos para los organismos con el fin de proteger los activos de información, frente a riesgos internos o externos que pudieran afectarlos, para preservar su confidencialidad, integridad y disponibilidad.
- Proteger los derechos de los titulares de los datos personales o los propietarios de la información.
- Proteger la información, los datos personales y los recursos informáticos de las organizaciones.

Directriz: política de seguridad de la información

Política de seguridad de la información: documento central para la protección de los datos y de los recursos utilizados para su tratamiento.

Esta política define la postura de una organización respecto al comportamiento que espera del personal y de terceros que tomen contacto con esos datos y/o recursos para protegerlos.

Es un conjunto de reglas, normas y protocolos de actuación elaborados para velar por la seguridad de la información y para protegerse de la delincuencia y de otros factores.

Directriz: política de seguridad de la información

Las organizaciones deben desarrollar una política de seguridad de la información que sea:

- ❑ compatible con la responsabilidad primaria y las acciones de su competencia.
- ❑ elaborada sobre la base de una evaluación de los riesgos que pudieran afectarlas.

Ese análisis permite valorar el costo de los posibles incidentes de seguridad que pueden afectar los activos de información, y priorizar las medidas que se tomarán para evitarlos.

<u>La política de seguridad debe ser:</u>

- ★ aprobada por las autoridades máximas del organismo u organización que la adopte.
- ★ notificada y cumplida por todo el personal.
- ★ revisada y actualizada cada 12 meses.
- ★ utilizada para establecer normas, procedimientos, y guías acordes a los procesos que se llevan adelante en la organización, su plataforma tecnológica y en otros recursos.

Directriz: aspectos organizativos de la seguridad

El organismo debe asignar a una área la responsabilidad de la seguridad de la información.
Se recomienda que la misma no dependa del sector de Sistemas o Tecnología de la Información.

Tendrá a su cargo la coordinación de todas las actividades tendientes a la implementación de la política de seguridad de la información.

También velará por la seguridad de la información en todos los proyectos y programas de la organización y por el establecimiento de procedimientos adecuados de seguridad, en base a un plan de tratamiento de riesgos.

Directriz: aspectos organizativos de la seguridad

-Impulsar desde la autoridad máxima las iniciativas del área de seguridad de la información tendientes a preservar la confidencialidad, integridad y disponibilidad de la información que se gestiona.

Confidencialidad

La información es accesible únicamente por el personal autorizado. Sólo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados a su acceso.

Ejemplos de falta de confidencialidad:
-el robo de información confidencial por parte de un atacante a través de Internet.
-la divulgación no autorizada de información confidencial a través de las redes sociales.
-el acceso de un empleado a información crítica de la compañía ubicada en carpetas sin permisos asignados.

Integridad

La integridad se refiere a que la información sólo sea creada, modificada o eliminada por aquella persona que esté autorizada a hacerlo.

Ejemplos de ataques contra la integridad:
- la alteración malintencionada en los ficheros del sistema informático mediante la explotación de una vulnerabilidad.
- la modificación de un informe importante por un empleado malintencionado o por un error humano.

Disponibilidad

La disponibilidad hace referencia a que la información esté accesible, disponible para nosotros en el formato y el momento que la necesitemos.

Ejemplos de falta de disponibilidad:
-cuando nos es imposible acceder al mail corporativo debido a un error de configuración.
-cuando se sufre un ataque de denegación de servicio y el sistema «cae» impidiendo accesos legítimos.

Directriz: aspectos organizativos de la seguridad

-Establecer mecanismos de seguridad para el trabajo remoto.

Este trabajo tiene hoy un uso pocas veces visto, en el que la inexperiencia y la necesidad de manejar nuevas herramientas sin el conocimiento adecuado puede ser explotada por ciberdelincuentes.

Riesgos que podemos correr

Virus, ransomware, phishing, interceptación de comunicación, robo o pérdida de los dispositivos, borrado o modificación de datos, pérdida de información, accesos indebidos a dispositivos, etc.

Ejemplos de medidas de seguridad

Videollamada: hacerla siempre desde el mismo lugar de la casa y, si es posible, usar un fondo virtual.

Directriz: aspectos organizativos de la seguridad

Si compartís capturas de pantalla o fotos de videoconferencias en redes sociales, pedí antes de hacerlo el consentimiento de los participantes.

No prestar dispositivos que pertenezcan a tu trabajo.

Usar siempre el mail institucional.

Comprobar que los antivirus estén actualizados.

-Establecer mecanismos de seguridad para el uso de dispositivos móviles según la criticidad de la información involucrada y de la jerarquía del trabajador.

Ejemplos de medidas de seguridad

Minimizar la cantidad de aplicaciones instaladas y descargarlas de tiendas oficiales.

Mantener actualizado el sistema operativo de los dispositivos y de todas las aplicaciones instaladas.

Descargar siempre las fotos y los documentos almacenados.

Activar el doble factor de autenticación para agregar una capa más de seguridad a las contraseñas.

Directriz: seguridad informática de los recursos humanos

El personal debe ser considerado un recurso central en las organizaciones y debe ser formado.

Todos deben ser concientizados y capacitados para desarrollar habilidades y conocimientos en seguridad de la información.

También se espera que logren hacer un uso responsable de la información y de los recursos usados en su gestión para prevenir riesgos.

Directriz: seguridad informática de los recursos humanos

-Implementar para todo el personal planes de concientización en el uso seguro y responsable de los activos de información.

-Promover el entrenamiento permanente de quienes desarrollan funciones en áreas de seguridad, tecnologías de la información, desarrollo de software e infraestructura.

-Suscribir actas o compromisos respecto a la seguridad de la información para todos los agentes de la organización, así como también acuerdos de confidencialidad.

-Establecer accesos a la información para cada perfil de trabajo.

Directriz: gestión de activos

Clasificar los activos de información en línea con la importancia de la información que gestionan para la organización.

Llevar un inventario actualizado en el que se detallen los datos para conocer la ubicación, el propietario y las responsabilidades correspondientes de cada activo.

Exigir al personal la devolución de los activos de información en su poder al finalizar la relación laboral o en un cambio de funciones.

Hacer una destrucción segura de cualquier medio que contenga información o datos personales, sobre un procedimiento documentado, una vez que no sirva más.

Directriz: autenticación, autorización y control de accesos

El acceso a los archivos y bases de datos de la organización debe ser otorgado formalmente a quienes lo requieran para sus funciones, es decir, para las actividades y tareas que cada empleado realice, con el fin de proveer un nivel apropiado de protección.

Así se evitarán errores como:

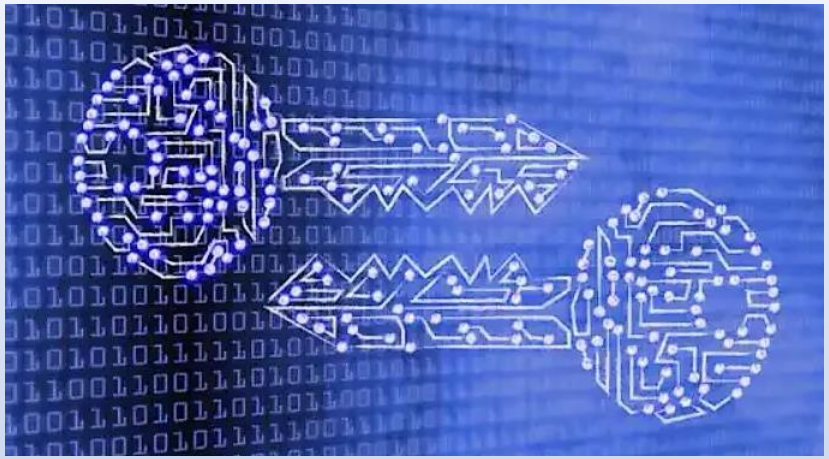
- Tener carpetas de red compartidas sin control de acceso.
- Que haya usuarios que no sepan dónde está la última versión de un documento.
- Que un usuario conserve acceso a información que ya no necesita, por un cambio de puesto.
- Que haya presencia de discos duros portátiles sin que la organización conozca y tenga inventariados quién los utiliza y qué información pueden tener almacenada.

Directriz: autenticación, autorización y control de accesos

Para cumplir con esta directriz, la norma dice que se debe:

- Utilizar el principio de “necesidad de saber”, es decir que solo se otorguen privilegios de acceso según las actividades y tareas que cada empleado deba llevar adelante.
- Gestionar las altas y bajas de cuentas de usuario y privilegios.
- Motivar el uso responsable de credenciales de acceso.
- Controlar y monitorear el uso responsable de los dispositivos, dejando sentado que se encuentra prohibido compartirlos y que deben ser mantenidos seguros.
- Revisar periódicamente todos los permisos de acceso a los sistemas y a la infraestructura de procesamiento.

Directriz: uso de herramientas criptográficas



La confidencialidad, integridad, autenticidad y/o no repudio de la información de la organización debe ser protegida mediante técnicas de cifrado, tanto si los datos se encuentran almacenados como cuando son transmitidos.

En este marco se debe:

- ❑ requerir el cifrado de cualquier dispositivo de la organización que contenga información considerada crítica y cuando involucre datos personales, especialmente, si este se lleva afuera de la institución.
- ❑ proteger adecuadamente los dispositivos y las claves criptográficas durante todo su ciclo de vida.
- ❑ utilizar certificados digitales en todos los sitios de Internet de la organización.

Directriz: seguridad física y ambiental

Los activos de información de la organización deben ser protegidos adoptando también recaudos físicos y ambientales para minimizar los riesgos asociados.

Esto implica, por ejemplo, lo siguiente:

- La protección de áreas seguras contra desastres naturales, ataques maliciosos o accidentales.
- La incorporación de controles físicos de ingreso y egreso.
- Tomar medidas de seguridad para que el equipamiento sea ingresado o retirado de la organización.
- Usar mecanismos de bloqueo de sesión y medidas para evitar la pérdida, daño o robo de la información.

Directriz: seguridad física y ambiental

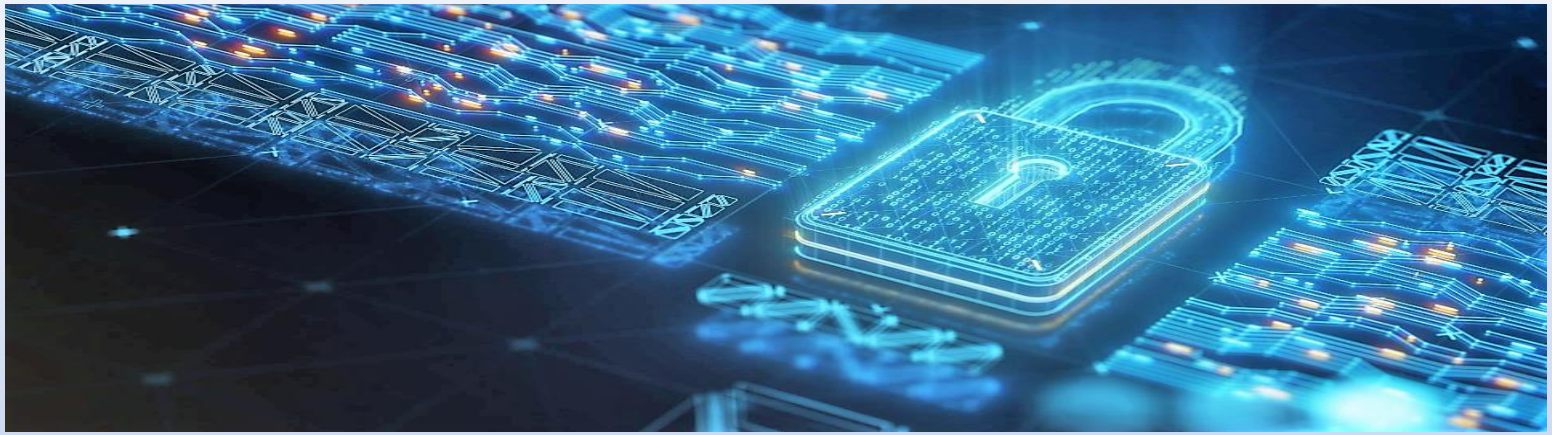
Ejemplos de medidas físicas para proteger la información

- Acondicionar adecuadamente la sala de servidores frente a riesgos de incendio, inundaciones o accesos no autorizados.
- Establecer un sistema de control de acceso para entrar en las oficinas.
- Poner cerraduras en los despachos y armarios.
- Guardar las copias de seguridad en una caja ignífuga.

Ejemplos de medidas técnicas

Son aquellas de carácter tecnológico que están dentro del ámbito de la seguridad, como la instalación de antivirus, cortafuegos, sistemas de copias de seguridad, entre otras.

Directriz: seguridad operativa



-Las operaciones de la organización deben hacerse de forma segura en todas las instalaciones de procesamiento de información, minimizando la pérdida o alteración de datos.

Para ello se debe:

Supervisar periódicamente la seguridad de los sistemas.

Proteger las instalaciones contra la intrusión de software malicioso.

Realizar copias de resguardo de los programas y de la información.

Identificar y gestionar las vulnerabilidades de los sistemas y las actualizaciones de software, etc.

Directriz: seguridad en las comunicaciones

La información de las redes debe ser protegida y controlada dentro de la organización y cuando es transferida fuera de las instalaciones de la misma.

Para tal fin, se recomienda:

- Exigir a todo el personal el uso del mail institucional para toda comunicación laboral.
- Incluir mecanismos que garanticen las transferencias seguras de datos (sistemas de cifrado, por ejemplo).
- Incorporar acuerdos y cláusulas de no divulgación y de confidencialidad, etc.

Directriz: adquisición, desarrollo y mantenimiento de sistemas de información

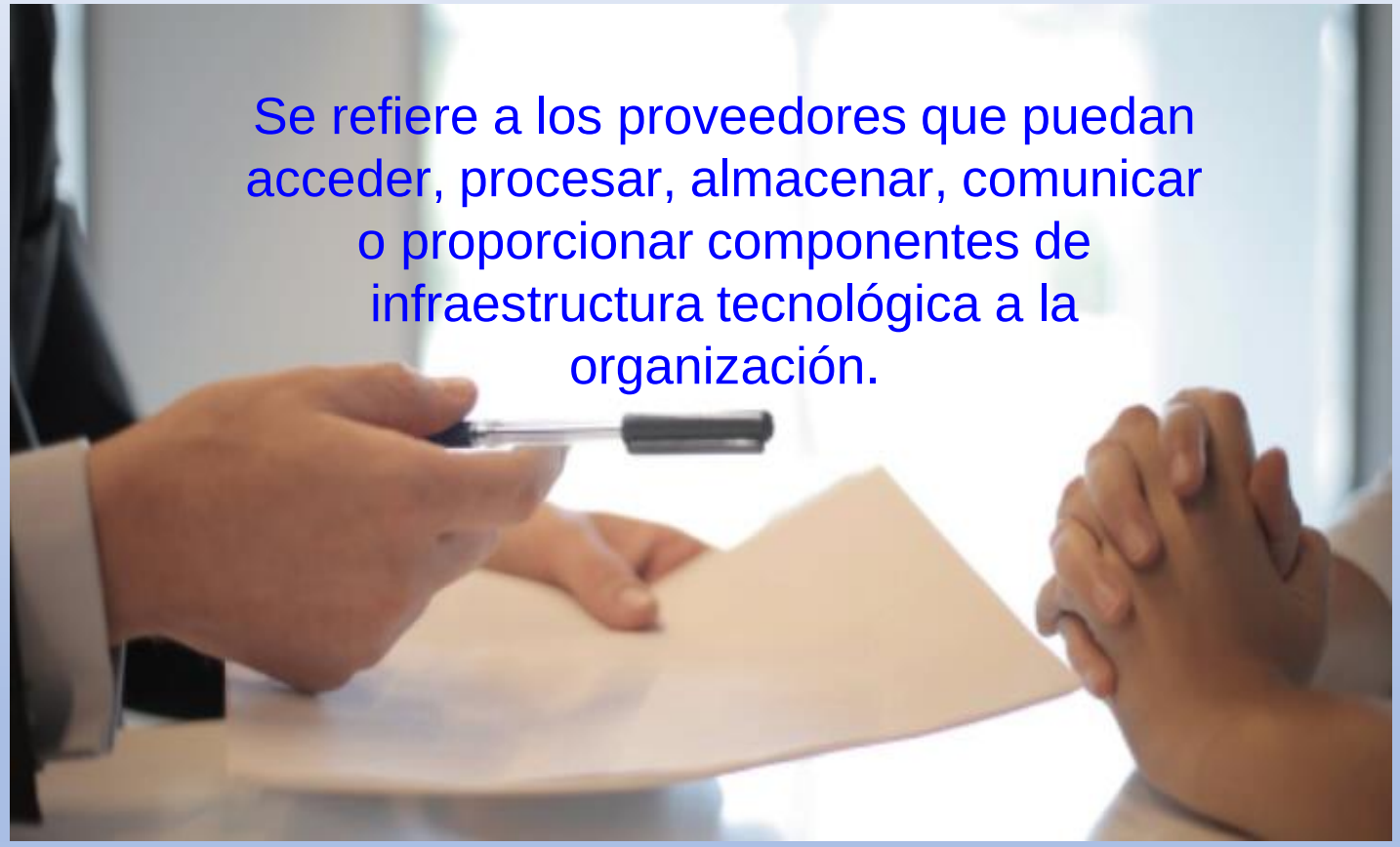
La seguridad de la información debe contemplarse como una parte integral de los sistemas de información, incluyendo aquellos que brinden servicios o permitan la realización de trámites a través de Internet.

-Proteger desde el diseño las aplicaciones que se desarrollen internamente, y utilizar una metodología de desarrollo seguro, por ejemplo, capacitando a los desarrolladores.
-Controlar los cambios que se realicen a las aplicaciones, implementando controles adecuados en las instancias de desarrollo, prueba y producción.
-La seguridad de las aplicaciones se debe evaluar antes de ponerlas productivas.

Directriz: relación con proveedores

La contratación, cualquiera sea la modalidad, realizada por la organización para la provisión de un bien o servicio debe incluir cláusulas relacionadas con la seguridad de la información.

Las mismas deben estar descritas en el pliego de bases y condiciones particulares, y deben ser de cumplimiento efectivo por parte del cocontratante desde el inicio del procedimiento contractual y hasta la finalización.



Gestión de incidentes de seguridad

La organización debe adoptar medidas para prevenir, detectar, gestionar, resolver y reportar incidentes de seguridad que puedan afectar sus activos de información.

Para tal fin, se debe:

Contar con procedimientos de gestión de incidentes de seguridad.

Instruir a los agentes para la prevención, detección y reporte de incidentes de seguridad.

Recopilar la evidencia necesaria para adoptar medidas administrativas o judiciales posteriores, cuidando la cadena de custodia.

Si el incidente de seguridad hubiere comprometido información y/o datos personales de terceros, se deberá informar públicamente tal ocurrencia.

¡Gracias!

Lic.Nancy Garnica
Mayo 2022

EXTRAIDO DE

JEFATURA.SANTACRUZ.GOB.AR/CIBERSEGURIDAD2022/