

Facultad de Tecnología Informática

# Seguridad Informática

**Trabajo Práctico Nº 01: Norma BCRA 4609**

Condiciones: Responda en base a la Norma con SUS PALABRAS. NO COPY / PASTE

**Grupo Rojo**

## **Alumnos**:

## Bárbara Covarrubias

## Otto Gonzalez

## Franco Fazzito

## Franco Balich

## Malena Aguillon

**Profesor**: Semería, Marcelo

**Fecha**: 25/8/2022

### ¿A quiénes apunta la Norma BCRA 4609?

**RTA:**

La norma BCRA 4609 está dirigida principalmente a las autoridades máximas de entidades financieras que operan en Argentina, que serán los responsables frente a cualquier incumplimiento de esta. Pero también, a los Comités de Tecnología Informática que serán instituidos por estos para la aplicación efectiva de la norma.

### ¿Quién es el responsable de fijar y mantener los niveles de seguridad física?

**RTA:**

El Directorio o alguna autoridad equivalente serán los responsables de la seguridad informática para proteger los recursos tecnológicos.

### ¿Qué características edilicias y de ubicación debe tener el centro de procesamiento de datos?

**RTA:**

El centro de datos como primera medida deberá localizarse en un área que resulte de difícil identificación pública. Hay que asegurar que es importante que el ambiente sea exclusivo, de manera que no pudieran quedar expuestas las operaciones críticas y de carácter confidencial de la entidad financiera a agentes externos.

Deben contar con niveles de protección físico-ambiental adecuados. Algunos de los siguientes se listan a continuación:

1. Instalaciones de montaje apropiadas para los sistemas de telecomunicaciones.
2. Instalaciones para equipo de apoyo (UPS, baterías, estabilizadores de tensión)
3. Instalaciones de montaje apropiadas para los sistemas de suministro eléctrico (primario y secundario).
4. Iluminación de emergencia

Además, los ambientes deben contar con un nivel de protección probadamente eficaz contra las amenazas de su entorno, con el fin de preservar la integridad tanto de los datos como del hardware.

### ¿Cuánto tiempo se deben mantener los informes realizados como control de gestión?

**RTA:**

En cuanto a esta pregunta, los informes realizados se deben mantener por 2 años. Si hacemos referencia a que la norma establece que los informes deben archivarse y conservarse por un plazo mínimo de dos años, período en el que podrán ser solicitados para su auditoría por parte de la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

### ¿Qué son los planes de continuidad? ¿Qué contienen? ¿Quién es el responsable? ¿Quién debe mantenerlos actualizados?

**RTA:**

Se llaman planes de continuidad a aquellas normas y procedimientos que deben de aplicarse al momento de que ocurra algún tipo de interrupción ya sea en los servicios como en sus operaciones normales.

Dichos procedimientos contienen las acciones y medidas necesarias para recuperar el servicio que se provee por Internet a los distintos usuarios.

Sera responsable la entidad, y en caso de haber delegado el servicio, dicha entidad debe exigir al delegado (un tercero) el cumplimiento de dicho plan de continuidad.

### ¿Qué es integridad? De un ejemplo en que no se cumpla y que se debe modificar para que se cumpla.

**RTA:**

La integridad de los datos consiste en la exactitud y fiabilidad de estos.

El objetivo de mantener la integridad es lograr que los datos ingresados, procesados y consolidados sean los correctos.

Un ejemplo de cómo buscar integridad es mediante el uso de firmas digitales.

En caso de que esta no se cumpla puede ser producto de una trama de datos no cumpla dicha firma es un indicio de que el contenido pudo haber sido alterado, y para hacer que dicho control se cumpla, debe verificarse estrictamente el certificado utilizado para la transacción.

### ¿Qué deben proteger las políticas de protección? ¿Quién las establece?

**RTA:**

Las políticas de restricción deben proteger principalmente los activos de información.

Estos activos son establecidos por el Directorio, o una autoridad equivalente dentro de la organización.

### ¿Qué es y por qué es necesaria la segregación de funciones? De un ejemplo.

**RTA:**

La segregación de funciones es la sectorización de las gerencias de tecnología, sistemas y/o desarrollo dentro de una entidad financiera o tercero que brinde servicios a la entidad, la misma es necesaria para prevenir incompatibilidades de funciones que puedan provocar un fraude, para ello se realizan controles cruzados por oposición de intereses.

Un ejemplo sencillo puede ser que aquella persona que desarrolla un módulo de extracción de dinero de una app bancaria, esa misma persona no debe ser la encargada de probarlo o de implementarlo en producción.

1. ¿Qué características deben tener las **contraseñas**? ¿Es obligatorio un cambio periódico?

**RTA:**

Las contraseñas se caracterizan por ser cambiadas o establecidas al primer ingreso para prevenir que se mantenga la contraseña por defecto que traen la mayoría de los dispositivos con el objetivo de evitar un posible acceso no autorizado al dispositivo debido a que las contraseñas por defecto son fácilmente deducibles si se conoce el fabricante del dispositivo en cuestión y asi asegurar la privacidad de los mensajes transmitidos.

Además, las contraseñas se caracterizan por tener como mínimo ocho caracteres de longitud y respetar determinadas reglas de formato para aumentar la dificultad del descifrado de las mismas por fuerza bruta. Inclusive no debe permitirse la repetición de alguna de las ultimas doce contraseñas utilizadas.

Su cambio es obligatorio y debe realizarse en un periodo de 30 días.

Aclaración: Estas políticas de seguridad normalmente se implementan en las políticas del dominio del usuario por ejemplo de Windows, obligándolo a realizar el cambio y que el mismo cumpla con la norma.

### Mencioné 5 buenas prácticas de seguridad. Justifique.

### RTA:

* + **Restricciones en el día y horario de los accesos:** Con el objetivo de prevenir que se realice un fraude un domingo donde puede no haber personal suficiente para mitigar el ataque o alertar el mismo.
  + **Bases de datos encriptadas:** Con el objetivo de mantener la privacidad de los datos de vital importancia para los clientes de una empresa, esto ayuda a evitar que la información contenida en ella se pueda usar para realizar un fraude. Esto se suele hacer en las bases de datos de las tarjetas de crédito.
  + **Prevenir accesos remotos** sin discriminar conexiones a la VPN que pueda producir que un antiguo empleado, un empleado nuevo o inclusive un empleado inexperto realice acciones desde un entorno menos controlado.
  + **Actualizaciones frecuentes de los sistemas operativos:** Con el objetivo de prevenir que alguna vulnerabilidad conocida sea aprovechada.
  + **Accesos biométricos:** Uso de huellas digitales para permitir el ingreso. lo que limita el acceso físico a personas con una huella.

### ¿Es obligatorio el uso de mecanismos biométricos?

**RTA:**

El uso de mecanismos biométricos no es obligatorio, pero si aporta un nivel más de seguridad al sistema, al igual que cualquier otra práctica que mejore la seguridad.

### ¿Cuáles son las funciones del Comité de Tecnología Informática?

**RTA:**

Las funciones del comité de tecnología informática son:

* Aprobación del plan estratégico de sistemas de información.
* Aprobación de la grades inversiones en tecnología de la información.
* Fijación de prioridades entre los grandes proyectos informáticos.
* Vinculo de discusión entre la informática y sus usuarios.
* Vigila y realiza el seguimiento de la actividad del departamento de informática.

### ¿De quién es la responsabilidad de controlar el desarrollo del Análisis de Riesgo?

**RTA:**

El Directorio o una autoridad equivalente, será el responsable de la existencia de mecanismos de control de grado de exposición a potenciales riesgos inherentes a los sistemas de información, de la tecnología informática y sus recursos asociados. Serán a la vez los responsables primarios de observar su continua ejecución.

### ¿Es obligatorio el uso de herramientas automatizadas para el análisis de la información contenida en los registros operativos, de seguridad y de auditoría?

**RTA:**

No lo es, sin embargo, se considera una buena práctica de seguridad, así como la detección en tiempo real de los eventos o instrucciones. De esta manera, se reducirá el volumen de los datos contenidos en los reportes, minimizando los costos relacionados con su almacenamiento y tareas de revisión.

### ¿Explique las ventajas y desventajas de vender los equipos de procesamiento que ya han dejado atrás su vida útil pero que funcionan correctamente?

**RTA:**

**Ventajas:**

* Los cambios tecnológicos suelen realizarse para que la empresa sea más moderna, que los procesos sean más rápidos, mayor productividad, competitividad en el mercado.
* Se pueden recuperar costos al vender equipos, que luego de su vida útil, permita recuperar parte la inversión realizada.
* Ahorro en costos de contratos extendidos destinados al soporte y mantenimiento de aquellos equipos que se deban mantener cuando el ciclo de vida del fabricante haya terminado.

### Desventajas:

* En caso de realizar un recambio de equipos, se debe realizar de forma controlada y cumpliendo la normativa vigente sobre los cambios.
* Los cambios de equipo consumen un determinado tiempo para la implementación de dichos cambios.
* La información contenida en equipos debe ser borrada a bajo nivel, evitando que el acreedor del equipo reciba algún dato sensible de la organización.

### ¿Qué utilidad tiene el inventario tecnológico? ¿Qué debe contener?

**RTA:**

El inventario tecnológico sirve como fuente de información para las entidades financieras. Gracias a esta información, se podrá asignar niveles de protección proporcionales a la importancia de activos, realizar una continua categorización de estos, mantenerlos actualizados y efectuar el mantenimiento preventivo de sus recursos físicos.

Las entidades financieras deben contar con la capacidad de identificar sus activos informáticos y de información, las características, localización y la criticidad e importancia de estos.

El inventario cómo mínimo debe tener los siguientes elementos:

* + Recursos de software: Software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.
  + Recursos de información: Bases de datos y archivos, documentación de sistemas, manuales de usuario, procedimientos operativos y/o soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia.
  + Activos físicos: Equipamiento informático (procesadores, monitores, módems, entre otros), equipos de comunicaciones (routers, firewalls, switches, encriptadores, etc.) medios magnéticos (cintas, discos), otros equipos técnicos.
  + Servicios descentralizados en terceros: Servicios informáticos y de comunicaciones, fábricas de software, otros.

### ¿Cuáles son las acciones mínimas que se deben considerar en el manejo de incidentes? Defina 3 acciones.

**RTA:**

Debe quedar como evidencia la existencia de procedimientos documentados para la gestión, acción y comunicación de problemas en sistemas productivos.

Como mínimo, se deben considerar las siguientes acciones:

* + Advertir y registrar los síntomas del problema y mensajes que aparecen en pantalla, fecha y hora del incidente.

Justificación: Ante posibles futuras auditorías, los datos recabados serán útiles para el rastreo y seguimientos de los problemas.

* + Dejar constancia de la comunicación a los sectores responsables de la resolución.

Justificación: Debe quedar un registro fiel de los sectores que son responsables de la participación en la resolución del problema.

* + Documentar accesiones realizas con fecha y hora de resolución.

Justificación: Tener una documentación de los problemas es útil, por un lado, para formar una base de conocimiento de la entidad financiera. Por otro lado, medir los tiempos de resolución de las fallas y su mejor de forma continua.

### ¿Forma parte el soporte a usuarios de las normas de seguridad?

**RTA:**

Si forma parte el soporte a usuarios de las normas de seguridad, específicamente en la sección de operaciones y procesamiento de datos se establece que debe existir un área o sector para el soporte, registro y seguimiento a los incidentes.

Esto con el objetivo de mantener un registro con los problemas que hayan surgido y demás incidentes relevantes, con los datos relevantes, el usuario, tipo y tiempo de resolución. Se deberán mantener por dos años estos registros en caso que sean requeridos por la Gerencia de Auditoría Externa de Sistemas de la Superintendencia de Entidades Financieras y Cambiarias.

### ¿Qué actividades pueden ser factibles de delegación y cuáles no? ¿Por qué? ¿Quién las define?

**RTA:**

Son factibles de delegación actividades vinculadas con la administración o procesamiento de datos, sistemas o tecnologías relacionadas, en las condiciones fijadas por la comunicación CREFI – capitulo 2 sección 6.

No pueden ser delegadas actividades con proveedores que a su vez tengan contratadas la función de auditar dichas actividades. Esto se debe a que no existiría un control correcto por oposición de intereses.

Las condiciones normativas y reguladoras sí serán exigibles y aplicables cuando se realicen en dependencias de terceros.

### ¿Qué aspectos se deben considerar en la documentación técnica?

**RTA:**

Deben considerarse aspectos tales como los objetivos, los alcances, los diagramas de sistema necesarios para interpretar la infraestructura y los sistemas que corren sobre la misma, inclusive bases de dato y manuales de usuario. También deben incluir el diseño de archivos y programas componentes de los sistemas.

Los manuales de usuarios finales de cada sistema aplicativo deben contemplar los mismos incisos: Objetivo, Alcance, descripción de funciones y menús, listado de controles e instrucciones para el caso de cancelaciones.