República Argentina - Poder Ejecutivo Nacional
2017 - Año de las Energías Renovables

Resolución General

Número: RESGC-2017-704-APN-DIR#CNV

CIUDAD DE BUENOS AIRES
Jueves 24 de Agosto de 2017

Referencia: Expediente Nº 1657/2017 “PROYECTO DE RG S/ CIBERSEGURIDAD Y RESILIENCIA CIBERNÉTICA”

VISTO el Expediente Nº 1657/2017 caratulado “PROYECTO DE RG S/ CIBERSEGURIDAD Y RESILIENCIA CIBERNÉTICA” del registro de la COMISIÓN NACIONAL DE VALORES, lo dictaminado por la Gerencia de Servicios Centrales, la Subgerencia de Verificaciones de Agentes y Mercados, la Subgerencia de Agentes y Calificadoras de Riesgo, la Gerencia de Agentes y Mercados, la Gerencia General de Mercados, la Subgerencia de Asesoramiento Legal, la Gerencia de Asuntos Jurídicos y la Gerencia General de Asuntos Jurídicos, y

CONSIDERANDO:

Que de acuerdo a las atribuciones otorgadas por el artículo 19 inciso g) de la Ley Nº 26.831, la COMISIÓN NACIONAL DE VALORES se encuentra facultada para dictar las normas a las cuales deben ajustarse los Mercados, los Agentes registrados y las demás personas físicas y/o jurídicas que por sus actividades vinculadas al Mercado de Capitales, y a criterio de la Comisión Nacional de Valores queden comprendidas bajo su competencia.

Que resulta conveniente adoptar estándares internacionales con respecto a la seguridad informática y atender a las recomendaciones de la ORGANIZACIÓN INTERNACIONAL DE COMISIONES DE VALORES (IOSCO, por sus siglas en inglés) sobre los principios de ciberseguridad y resiliencia cibernética.

Que el Comité de Sistemas de Pago y Liquidación (CPSS) del Banco de Pagos Internacionales (BIS) y el Comité Técnico de IOSCO establecen a través de los “Principios Básicos para Infraestructuras de Mercado Financiero” que las “Infraestructuras de Mercado Financiero” cumplen un rol crítico en el sistema financiero y en la economía en general.

Que los principios mencionados enumeran las principales categorías de riesgos identificados y proporcionan orientación a las “Infraestructuras de Mercado Financiero” y a las autoridades competentes sobre la identificación, monitoreo, mitigación y administración de estos riesgos.

Que asimismo, definen los riesgos operacionales como la posibilidad de que deficiencias en los sistemas de información y en los procesos internos, errores humanos y/o fallas por eventos externos, resulten en la

reducción, deterioro o interrupción de los servicios proporcionados por una “Infraestructura de Mercado Financiero”.

Que la interoperabilidad de las infraestructuras críticas del Mercado de Capitales posibilitaría la propagación y ampliación de los efectos de los ciberataques, así como las vías de acceso de amenazas, aumentando el riesgo sistémico.

Que al respecto, el Comité de Pagos e Infraestructuras de Mercado (CPMI – ex CPSS) del BIS junto con el Directorio de IOSCO elaboraron una “Guía sobre la Resiliencia Cibernética para las Infraestructuras de Mercado Financiero”, con la finalidad de proporcionar orientación a las “Infraestructuras de Mercado Financiero” para mejorar su gestión sobre los riesgos cibernéticos, destacando que el nivel de respuesta a los incidentes de seguridad contribuye a conservar su capacidad operativa.

Que el mencionado documento proporciona recomendaciones tendientes a ampliar la capacidad de resiliencia cibernética de las “Infraestructuras de Mercado Financiero”, alineadas con los controles y buenas prácticas definidas por el estándar de la familia ISO 27000, como estrategias utilizadas internacionalmente para mitigar los riesgos relativos a la ciberseguridad.

Que, adicionalmente, el desarrollo asimétrico respecto a las tecnologías de la información de los distintos actores del Mercado de Capitales, torna necesario un plan de implementación diferenciado según el grado de madurez de los mismos.

Que la presente Resolución General se dicta en ejercicio de las atribuciones conferidas por el artículo 19 inciso g) de la Ley N° 26.831.

Por ello,

LA COMISIÓN NACIONAL DE VALORES

RESUELVE:

ARTÍCULO 1°.- Incorporar como Sección VII del Capítulo III del Título VI de las NORMAS (N.T. 2013 y mod.), el siguiente texto:

“SECCIÓN VII.

CIBERSEGURIDAD Y CIBERRESILIENCIA CRÍTICAS DEL MERCADO DE CAPITALES.

ARTÍCULO 20.- El órgano de administración de los Mercados, Agentes de Depósito Colectivo, Cámaras Compensadoras y Agentes de Custodia, Registro y Pago, deberá, antes del 1° de enero de 2018, aprobar las “Políticas de Seguridad de la Información” elaboradas conforme los lineamientos de la norma ISO 27000, según el Anexo del presente Capítulo, titulado “Ciberseguridad y Ciberresiliencia de las Infraestructuras Críticas del Mercado de Capitales”.

ARTÍCULO 21.- Dentro de los DOS (2) meses de aprobadas, por el órgano de administración, las “Políticas de Seguridad de la Información”, los sujetos mencionados en el artículo anterior deberán elaborar un “Plan de Implementación de las Políticas de Seguridad de la Información del Mercado de Capitales” a través de procedimientos que incorporen un criterio de mejora continua.

ARTÍCULO 22.- Las “Políticas de Seguridad de la Información” deberán aplicarse a los activos informáticos y a los procesos relacionados a la prestación de servicios esenciales.

ARTÍCULO 23.- Los sujetos mencionados en el artículo 20 deberán antes del 1° de marzo de 2018, adoptar

medidas, de resiliencia cibernética, siguiendo los lineamientos de la “Guía sobre la Resiliencia Cibernética para las Infraestructuras de Mercado Financiero” de la CPSS - IOSCO.

ARTÍCULO 24.- El informe de auditoría externa anual de sistemas que deben remitir los sujetos mencionados en el artículo 20, adicionalmente deberá contener la opinión del auditor respecto del “Plan de Implementación de las Políticas de Seguridad de la Información del Mercado de Capitales”, incluyendo el grado de avance en el desarrollo del mismo y de cumplimiento de los objetivos de control requeridos en el Anexo titulado “Ciberseguridad y Ciberresiliencia de las Infraestrucuturas críticas del Mercado de Capitales”.

ARTÍCULO 2°.- Incorporar como Anexo del Capítulo III del Título VI de las NORMAS (N.T. 2013 y mod.), el siguiente texto:

“ANEXO

Ciberseguridad y Ciberresiliencia de las Infraestructuras críticas del Mercado de Capitales.

CONTENIDO.

SECCIÓN I

Políticas de tecnología de la información, comunicaciones y seguridad.

Orientación de la Dirección para la seguridad de la información.

Políticas de seguridad y gestión de la información.

Revisión de las políticas.

Comité de tecnología/seguridad con participación del Directorio.

Plan y presupuesto de seguridad y ti.

SECCIÓN II

Roles y responsabilidades.

Responsabilidad de la Dirección.

Roles y responsabilidades de seguridad de la información.

Segregación de funciones.

Contacto con las autoridades.

Contacto con grupos de interés especial.

Seguridad de la información en la gestión de proyectos.

SECCIÓN III

Capital Humano.

Evaluación previa al ingreso.

15.1. Investigación de antecedentes.

15.2. Términos y condiciones de empleo.

Seguimiento de la relación laboral.

16.1. Responsabilidades de la Dirección.

16.2. Concientización, educación y capacitación en seguridad de la información.

Finalización del vínculo laboral.

17.1 Responsabilidades en la desvinculación o cambio de puesto.

SECCIÓN IV

Activos de la información.

Identificación.

Inventario de los activos.

Propiedad de los activos.

Uso aceptable de los activos.

Retorno de los activos.

Clasificación de la información.

Metodología para el análisis de riesgos informáticos.

Manipulación de los activos.

SECCIÓN V

Usuarios de la información.

Política de control de accesos.

Requisitos del negocio para el control de accesos a los sistemas y las aplicaciones.

Acceso a las redes y a los servicios de red.

Gestión de accesos del usuario.

Alta y baja de registros de usuario.

Gestión de los derechos de acceso privilegiado.

Revisión de los derechos de acceso del usuario.

Remoción o ajuste de los derechos de acceso.

Procedimientos seguros de inicio de sesión.

Sistema de gestión de autenticación.

SECCIÓN VI

Seguridad de la infraestructura.

Áreas Seguras.

38.1. Perímetro de seguridad física.

38.2. Controles físicos.

38.3. Aseguramiento de oficinas, recintos e instalaciones.

38.4. Protección contra amenazas externas y del entorno.

Equipamiento.

39.1. Ubicación y protección del equipamiento.

39.2. Mantenimiento del equipamiento.

39.3. Retiro de activos.

39.4. Disposición final segura o reutilización del equipamiento.

Dispositivos móviles y teletrabajo.

40.1. Política de dispositivo móvil.

40.2. Teletrabajo.

SECCIÓN VII

Gestión de operaciones.

Procedimientos operativos documentados.

Gestión de la capacidad.

Controles contra código malicioso.

Resguardo de la información.

Registro de eventos.

Protección de la información de los registros.

Control de las vulnerabilidades técnicas.

SECCIÓN VIII

Gestión de comunicaciones.

Gestión de la seguridad de la red.

52.1. Controles de red.

52.2. Seguridad de los servicios de red.

52.3. Segregación en redes.

SECCIÓN IX

Gestión de plataformas productivas.

Generalidades.

Gestión de requerimientos y requisitos de seguridad/controles.

Desarrollo seguro.

Separación de entornos de desarrollo, prueba y producción .

Pruebas.

Paquetes de software y desarrollo tercerizado.

SECCIÓN X

Relaciones con proveedores.

Seguridad de la información en las relaciones con los proveedores .

Política de seguridad de la información para las relaciones con los proveedores.

Tratamiento de la seguridad en los acuerdos con los proveedores.

Cadena de suministro de las tecnologías de la información y las comunicaciones.

Gestión de la entrega de servicios prestados por los proveedores.

Seguimiento y revisión de los servicios prestados por los proveedores.

SECCIÓN XI

Monitoreo.

Responsabilidades y procedimientos .

Presentación de informes sobre los eventos de seguridad de la información.

Presentación de informes sobre las vulnerabilidades de seguridad de la información.

Evaluación y decisión sobre los eventos de seguridad de la información.

Respuesta a los incidentes de seguridad de la información.

Aprendizaje a partir de los incidentes de seguridad de la información.

Recolección de la evidencia.

SECCIÓN XII

Gestión de continuidad del negocio

Gestión de la continuidad.

Planificación de la continuidad del negocio.

Implementación de plan de contingencia.

Implementación de la continuidad del negocio.

Prueba del plan de continuidad.

Verificación, revisión y valoración de la continuidad del negocio.

Redundancias.

SECCIÓN XIII

Relación con otras partes interesadas.

Ecosistema.

Canal de contacto.

Documentación de interconexiones.

Identificación de riesgos.

Pruebas conjuntas.

Ambiente de pruebas.

Control de cambios.

Acuerdos de intercambio de información.

Detección de vulnerabilidades.

Respuestas ante incidentes.

Sincronización de relojes.

SECCIÓN I

POLÍTICAS DE TECNOLOGÍA DE LA INFORMACIÓN, COMUNICACIONES Y SEGURIDAD.

ORIENTACIÓN DE LA DIRECCIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN.

ARTÍCULO 1º.- La Dirección debe establecer el marco de gobierno de resiliencia de ciberseguridad en el que se establezcan los lineamientos para la gestión de la tecnología, las comunicaciones y la seguridad de la información, con el objetivo de asegurar el negocio y la continuidad de operaciones de los Mercados, Agentes de Depósito Colectivo, Cámaras Compensadoras, y Agentes de Custodia, Registro y Pago (*CMI "capital market integration"*).

ARTÍCULO 2º.- El marco de resiliencia de la ciberseguridad debe estar alineado con los requisitos del negocio y orientado a formalizar el apoyo de parte de la Dirección. Este apoyo debe ser tomado como referencia por todo el personal involucrado en el diseño, implementación y revisión del proceso.

La Dirección debe definir la tolerancia de riesgo y es responsable de aprobar periódicamente el marco de resiliencia de la ciberseguridad, para asegurar que el riesgo definido es consistente con los objetivos de

negocio.

POLÍTICAS DE SEGURIDAD Y GESTIÓN DE LA INFORMACIÓN

ARTÍCULO 3º.- Se debe contar con políticas de seguridad y gestión de la información aprobada por la Dirección.

Las políticas deben ser publicadas y conocidas por todos los miembros de la organización; y deben definir y asignar claramente las responsabilidades de los distintos sectores sobre los activos informáticos, considerando las siguientes premisas:

- Los requisitos de negocio y funcionales de los sistemas de información serán definidos por los usuarios propietarios de los datos.

- La gestión de los activos tecnológicos que soportan la automatización de los procesos críticos será de exclusiva responsabilidad de las áreas de TI:

Activos físicos: equipos de procesamiento, comunicaciones y almacenamiento de la información, y su infraestructura relacionada.

Activos de software de base: sistemas operativos, motores de bases de datos, herramientas de desarrollo, etc.

ARTÍCULO 4º.- El responsable de Seguridad de la Información debe tener suficiente autoridad, independencia, recursos y acceso al Directorio. Dicho ejecutivo debe poseer la experiencia y los conocimientos necesarios para planificar y ejecutar las iniciativas de resiliencia de ciberseguridad, de manera competente, adicionalmente será responsable de la gestión de los activos relacionados con su función.

ARTÍCULO 5º.- Para la implementación de cualquier nuevo aplicativo, las áreas usuarias y técnicas (TI y Seguridad Informática) deberán trabajar coordinadamente para encontrar la solución adecuada (ya sea un paquete de software de terceros o una aplicación desarrollada internamente) que satisfaga los requisitos de negocio definidos por los usuarios y cumpla simultáneamente los estándares tecnológicos y de seguridad determinados por los responsables técnicos.

REVISIÓN DE LAS POLÍTICAS

ARTÍCULO 6º.- Las políticas de seguridad de la información deben ser revisadas al menos una vez por año (o antes si ocurren cambios significativos) para validar que continúan siendo apropiadas, adecuadas y eficaces en relación a los objetivos del negocio.

COMITÉ DE TECNOLOGÍA/SEGURIDAD CON PARTICIPACIÓN DEL DIRECTORIO

ARTÍCULO 7º.- Se debe conformar un comité de tecnología/seguridad en el cual la Dirección sea responsable de establecer, aprobar y velar por la actualización de un marco para fortalecer la ciberseguridad, incluyendo la responsabilidad por la toma de decisiones para la gestión de riesgos cibernéticos, incluso en situaciones de emergencia y de crisis.

La alta gerencia debe supervisar estrechamente la aplicación de su marco de resiliencia de la ciberseguridad como así también las políticas, procedimientos y controles que lo soportan.

PLAN Y PRESUPUESTO DE SEGURIDAD Y TI.

ARTÍCULO 8º.- De acuerdo con las metas y planes estratégicos, se deben elaborar planes operativos que contemplen los factores críticos para un efectivo control sobre los sistemas y la seguridad de la

información, junto con las actividades del negocio que respaldan. Dichos planes tendrán en cuenta las tareas a realizar con su correspondiente asignación de tiempos y recursos, los presupuestos, las prioridades y la precedencia de cada una de ellas.

SECCIÓN II

ROLES Y RESPONSABILIDADES.

RESPONSABILIDAD DE LA DIRECCIÓN.

ARTÍCULO 9º.- La Dirección es responsable de promover una adecuada administración de la seguridad de la información y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN.

ARTÍCULO 10.- Se deben definir y asignar claramente las responsabilidades relativas a la seguridad de la información.

SEGREGACIÓN DE FUNCIONES.

ARTÍCULO 11.- Las funcionalidades y responsabilidades en conflicto deben estar separadas con el fin de reducir los riesgos de modificaciones no intencionales o no autorizadas, o el mal uso de activos de información.

CONTACTO CON LAS AUTORIDADES.

ARTÍCULO 12.- Se deben mantener los contactos apropiados con las autoridades pertinentes.

CONTACTO CON GRUPOS DE INTERÉS ESPECIAL.

ARTÍCULO 13.- Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.

SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.

ARTÍCULO 14.- La seguridad de la información se contempla en la dirección de proyectos, independientemente del tipo de proyecto.

SECCIÓN III

CAPITAL HUMANO.

EVALUACIÓN PREVIA AL INGRESO.

ARTÍCULO 15.- Se debe asegurar que los empleados y contratados entiendan sus responsabilidades y sean idóneos para los roles para los cuales se los contrata.

15.1. INVESTIGACIÓN DE ANTECEDENTES.

Se debe realizar la verificación de antecedentes de todos los candidatos para el empleo de acuerdo con las leyes, regulaciones y reglas éticas pertinentes. Dicha verificación debe ser proporcional a los requisitos de seguridad de la organización, a la clasificación de la información a ser accedida y a los riesgos potenciales percibidos.

15.2. TÉRMINOS Y CONDICIONES DE EMPLEO.

Los contratos con empleados y contratados deben establecer sus responsabilidades y las de la organización para con la seguridad de la información.

SEGUIMIENTO DE LA RELACIÓN LABORAL.

ARTÍCULO 16.- Se debe asegurar que los empleados y contratados sean conscientes de sus responsabilidades con respecto a la seguridad de la información y las cumplan. Los recursos humanos deben mantenerse técnicamente capacitados e informados conforme a la evolución de los requerimientos, normas y tecnologías de los sistemas de seguridad adoptados por las organizaciones.

16.1. RESPONSABILIDADES DE LA DIRECCIÓN.

La Dirección y las gerencias deben requerir a todos los empleados y contratados que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.

16.2. CONCIENTIZACIÓN, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN.

Todos los empleados de la organización y, cuando sea pertinente los proveedores, deben recibir una concientización, educación y capacitación apropiada como así también actualizaciones regulares sobre las políticas y procedimientos organizacionales relativos a su tarea.

FINALIZACIÓN DEL VÍNCULO LABORAL.

ARTÍCULO 17.- Se deben proteger los intereses de la organización como parte del proceso de desvinculación o cambio de puesto.

17.1 RESPONSABILIDADES EN LA DESVINCULACIÓN O CAMBIO DE PUESTO.

Se deben definir, comunicar y hacer cumplir, al empleado o contratado, las responsabilidades y obligaciones relativas a la seguridad de la información que continúen vigentes luego de la desvinculación o cambio de puesto. Se debe verificar que las asignaciones, atribuciones y accesos a la información se actualicen debidamente ante cambios de funciones o desvinculaciones.

SECCIÓN IV

ACTIVOS DE LA INFORMACIÓN.

IDENTIFICACIÓN.

ARTÍCULO 18.- La organización debe tener un conocimiento preciso sobre los activos que posee, logrando y manteniendo una apropiada protección de los mismos.

Se define como activo a la información crítica de negocio y todas aquellas plataformas que procesan, almacenan y transmiten dicha información.

INVENTARIO DE LOS ACTIVOS.

ARTÍCULO 19.- La organización debe identificar los activos relevantes en el ciclo de vida de la información e inventariarlos para su control. El inventario deberá ser actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad al menos anual.

PROPIEDAD DE LOS ACTIVOS.

ARTÍCULO 20.- Se debe implementar un proceso para la asignación de un propietario de los activos

organizacionales. La propiedad debe ser asignada ante la creación, desarrollo o adquisición de los mismos. El propietario debe ser responsable de la gestión adecuada de un activo durante todo su ciclo de vida y responsable de su clasificación.

USO ACEPTABLE DE LOS ACTIVOS.

ARTÍCULO 21.- La autoridad relevante deberá identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados.

Los empleados y usuarios externos que utilicen o tengan acceso a los activos de la organización deberán estar informados de los requisitos de seguridad de la información, de los activos de la organización asociados con las instalaciones, recursos y procesamiento de información.

RETORNO DE LOS ACTIVOS.

ARTÍCULO 22.- Todos los empleados y usuarios externos deben devolver todos los activos de la organización en su poder al finalizar su empleo, contrato o acuerdo. El proceso de terminación debe formalizarse para incluir la devolución de todos los activos físicos y electrónicos pertenecientes a la organización.

CLASIFICACIÓN DE LA INFORMACIÓN.

ARTÍCULO 23.- Con el objetivo de asegurar que la información reciba un nivel de protección apropiado, la misma debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado en su gestión.

Las clasificaciones y los controles de protección asociados a la información deben tener en cuenta las necesidades del negocio de compartirla o restringirla, así como los requisitos legales.

Los resultados de la clasificación deben ser actualizados de acuerdo con los cambios de su valor, sensibilidad y criticidad a través de su ciclo de vida.

ARTÍCULO 24.- Para clasificar un activo de información, se deben evaluar las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

Se considera críticos como mínimo a aquellos activos de la información relacionados con las operaciones, saldos, movimientos, cuentas, comitentes y garantías de sus Mercados como así también de otros Mercados.

METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS INFORMÁTICOS.

ARTÍCULO 25.- Se debe evidenciar la existencia de análisis de riesgos formalmente realizados y documentados sobre los sistemas de información, la tecnología informática y sus recursos asociados.

Los resultados de los análisis mencionados y sus actualizaciones periódicas deben ser formalmente reportados al Comité de Tecnología/Seguridad, que será el responsable primario de darle tratamiento a las debilidades que expongan a los CMI a un riesgo mayor al aceptable.

MANIPULACIÓN DE LOS ACTIVOS.

ARTÍCULO 26.- Para cada uno de los niveles de clasificación, se deben definir los procedimientos de manejo seguro, incluyendo las actividades de procesamiento, almacenamiento, transmisión, clasificación y destrucción.

SECCIÓN V

USUARIOS DE LA INFORMACIÓN.

POLÍTICA DE CONTROL DE ACCESOS.

ARTÍCULO 27.- Se debe formalizar una política de control de accesos alineada a los requisitos del negocio acorde a la clasificación de activos definida en los ARTÍCULOS 23 y 24.

REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESOS A LOS SISTEMAS Y LAS APLICACIONES.

ARTÍCULO 28.- La organización debe basar las restricciones de acceso a la información en los requisitos de las aplicaciones individuales y de acuerdo con la política de control de acceso.

Con el objetivo de proteger la información relativa al negocio, se debe limitar al mínimo el acceso a la información crítica.

ACCESO A LAS REDES Y A LOS SERVICIOS DE RED.

ARTÍCULO 29.- Se debe permitir el acceso solamente a aquellos usuarios que cuenten con la debida autorización y hayan sido apropiadamente capacitados. La autorización debe ser acorde al rol desempeñado en el negocio.

GESTIÓN DE ACCESOS DEL USUARIO.

ARTÍCULO 30.- Se debe asegurar el acceso solamente a los usuarios autorizados, teniendo en cuenta las funciones de desarrollo, procesamiento y operación de los sistemas afectados, manteniendo siempre los principios de confidencialidad, integridad y disponibilidad.

ALTA Y BAJA DE REGISTROS DE USUARIO.

ARTÍCULO 31.- Se debe implementar un proceso formal de alta, baja y modificación de roles y permisos del usuario, formalizando el proceso de asignación de accesos. En la medida de lo posible, se debe establecer una línea base de configuración de seguridad y forzarla en todos los sistemas críticos.

GESTIÓN DE LOS DERECHOS DE ACCESO PRIVILEGIADO.

ARTÍCULO 32.- Se deben identificar los grupos de usuarios con permisos elevados en los diferentes dispositivos y sistemas críticos, para luego controlar la asignación y utilización de sus derechos de acceso sobre los mismos.

ARTÍCULO 33.- Debe restringirse, controlarse rigurosamente y segregarse adecuadamente el uso de herramientas con privilegios que podrían ser capaces de anular los controles en los sistemas, o que permitan el alta, baja o modificación de datos operativos por fuera de las aplicaciones.

REVISIÓN DE LOS DERECHOS DE ACCESO DEL USUARIO.

ARTÍCULO 34.- Se debe establecer un proceso de revisión periódica de los accesos otorgados a los usuarios para los dispositivos, herramientas y sistemas críticos, en el cual deben participar los propietarios de los activos y responsables del negocio. Este proceso debe realizarse como mínimo una vez por año, o antes si existiera alguna situación que lo justifique.

REMOCIÓN O AJUSTE DE LOS DERECHOS DE ACCESO.

ARTÍCULO 35.- En el caso de cambio de roles o desvinculación de usuarios, se deben revisar y ajustar los derechos de acceso a los servicios y sistemas a los cuales tenía acceso, y luego aplicar los cambios que sean necesarios. Este proceso debe estar validado por los propietarios de activos o responsables del negocio.

PROCEDIMIENTOS SEGUROS DE INICIO DE SESIÓN.

ARTÍCULO 36.- El procedimiento para iniciar sesión en un sistema o aplicación debe ser diseñado para reducir al mínimo la oportunidad de que ocurra un acceso no autorizado, incluyendo la selección de técnicas de autenticación adecuadas para demostrar la identidad alegada de un usuario. La cantidad y fortaleza de los métodos de autenticación empleados debe ser acorde con el tipo de información a proteger y los riesgos identificados. En particular, las organizaciones deben establecer fuertes controles sobre accesos privilegiados mediante su limitación y supervisión estricta.

Cuando el nivel de riesgo lo amerite, se analizará el empleo de más de un método de autenticación como contraseñas, tarjetas inteligentes, tokens o medios de reconocimiento biométricos.

Para los accesos iniciados desde ubicaciones externas a la infraestructura de la organización, ya sean propias o contratadas a un tercero, se deberá considerar más de un mecanismo de autenticación para el inicio de sesión.

SISTEMA DE GESTIÓN DE AUTENTICACIÓN.

ARTÍCULO 37.- La administración de la información para la autenticación debe considerar los siguientes aspectos:

- Cambiar los datos de autenticación por defecto de todos los productos instalados.

- Evitar el uso de cuentas genéricas, imponiendo identificadores de usuario y datos de autenticación individuales con el objetivo de posibilitar la rendición de cuentas y los análisis forenses.

- Proteger el almacenamiento y la transmisión de los datos de autenticación a través de algoritmos criptográficos reconocidos internacionalmente.

- Solicitar a los usuarios su autenticación luego de 15 minutos de inactividad.

- En caso de extravío del medio de autenticación debe existir un proceso de bloqueo del utilizado y validación para la entrega del nuevo medio.

Adicionalmente, si el medio de autenticación utilizado es a través de contraseñas se deben considerar los siguientes aspectos:

- Obligar a los usuarios a cambiar sus contraseñas en la primera conexión.

- Permitir a los usuarios seleccionar y cambiar sus propias contraseñas, considerando las siguientes características: longitud mínima de 8 caracteres cuya composición debe incluir caracteres numéricos, alfanuméricos y especiales, evitando la reutilización de las últimas 12 contraseñas.

- Forzar cambios periódicos de contraseña como mínimo cada 90 días.

- Implementar medidas técnicas para mitigar ataques del tipo “diccionario” o “fuerza bruta” tales como bloqueo de cuenta luego de una cierta cantidad de intentos fallidos de inicio de sesión, captchas, delays o requerimiento de autenticación de 2 factores.

SECCIÓN VI

SEGURIDAD DE LA INFRAESTRUCTURA.

ÁREAS SEGURAS

ARTÍCULO 38.- Se deben proteger las instalaciones e infraestructuras de procesamiento contra daños y

accesos no autorizados.

38.1. PERÍMETRO DE SEGURIDAD FÍSICA.

Se deben utilizar perímetros de seguridad para proteger áreas que contengan información e instalaciones de procesamiento de información sensibles o críticas. El Directorio o autoridad equivalente, es el responsable primario por la existencia de distintos niveles de seguridad física en correspondencia con el valor, confidencialidad y criticidad de los recursos a proteger y los riesgos identificados.

38.2. CONTROLES FÍSICOS.

Deberán protegerse las áreas seguras mediante controles apropiados, por lo que se deben considerar, entre otras, las siguientes medidas de prevención y control:

- Instalaciones para equipamientos de apoyo, tales como equipos de aire acondicionado, grupos generadores, llaves de transferencia automática, UPS, baterías, estabilizadores y tableros de distribución de energía y de telecomunicaciones.

- Instalaciones de montaje apropiadas para los sistemas de telecomunicaciones.

- Instalaciones de montaje apropiadas para los sistemas de suministro eléctrico, tanto primario como secundario.

- Iluminación de emergencia.

- Sistemas de monitoreo y control de las utilidades críticas del centro de procesamiento de datos.

- Controles de acceso, por medio de los cuales se permita sólo el ingreso al área de procesamiento de datos a personal autorizado.

Todos los accesos, de rutina o de excepción, deben ser registrados por mecanismos que permitan la posterior revisión de al menos los siguientes datos: nombre completo, relación (interno o externo), en caso de ser externo deberá constar quién ha autorizado el acceso, motivo, hora de ingreso y hora de egreso.

Los sistemas de prevención contra incendios en los ambientes de procesamiento de datos deben posibilitar alarmas preventivas, que tengan la capacidad de ser disparadas automáticamente ante la presencia de partículas características en el recalentamiento de materiales eléctricos y otros materiales combustibles presentes en las instalaciones.

Los materiales combustibles deben ser minimizados dentro del área del centro de procesamiento de datos. La mampostería, muebles y útiles deben ser constructivamente no inflamables, y preferentemente ignífugos.

Para el caso de que este servicio sea provisto por terceros se deberá solicitar al proveedor cumplir con lo exigido en la sección X.

38.3. ASEGURAMIENTO DE OFICINAS, RECINTOS E INSTALACIONES.

Deben diseñarse y aplicarse controles de seguridad física para oficinas, recintos e instalaciones, proporcionales a su criticidad y a los riesgos identificados.

38.4. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y DEL ENTORNO.

Se deben diseñar y aplicar medidas de protección física contra desastres naturales, ataques intencionales o accidentes.

EQUIPAMIENTO.

ARTÍCULO 39.- Se debe proteger el equipamiento (de procesamiento de la información y de soporte) de la organización contra daño, pérdida o robo.

39.1. UBICACIÓN Y PROTECCIÓN DEL EQUIPAMIENTO.

Se debe proteger el equipamiento de manera tal que se reduzcan los riesgos por amenazas y peligros del entorno, y las oportunidades de acceso no autorizado.

Dicho equipamiento se debe proteger de fallas causadas por el suministro eléctrico o de otras interrupciones ocasionadas por fallas en elementos de soporte.

39.2. MANTENIMIENTO DEL EQUIPAMIENTO.

El equipamiento debe recibir un mantenimiento correcto y oportuno para asegurar su continua disponibilidad e integridad.

39.3. RETIRO DE ACTIVOS.

Debe evitarse el retiro sin previa autorización del equipamiento o información en diferentes medios, tanto digitales como físicos, utilizados en las oficinas como en los centros de procesamiento. En caso de tratarse de datacenters de terceros el personal autorizado a retirar equipamiento deberá registrarlo para su posterior control.

Se deben aplicar medidas de seguridad a los activos en tránsito o fuera de la organización, considerando los diversos riesgos de operar fuera de sus instalaciones.

39.4. DISPOSICIÓN FINAL SEGURA O REUTILIZACIÓN DEL EQUIPAMIENTO.

Se deben verificar todos los componentes del equipamiento que contengan medios de almacenamiento para asegurar que, antes de su disposición final o reutilización, se haya eliminado o sobrescrito de manera segura cualquier dato sensible y software licenciado.

DISPOSITIVOS MÓVILES Y TELETRABAJO.

ARTÍCULO 40.- Se deben considerar los riesgos específicos del teletrabajo y la utilización de dispositivos móviles.

40.1. POLÍTICA DE DISPOSITIVO MÓVIL.

Se debe adoptar una política de soporte y medidas de seguridad para gestionar los riesgos introducidos mediante el uso de dispositivos móviles.

40.2. TELETRABAJO.

Se debe adoptar una política de soporte y medidas de seguridad destinadas a proteger la información accedida, transferida o almacenada en los sitios de teletrabajo.

SECCIÓN VII

GESTIÓN DE OPERACIONES.

PROCEDIMIENTOS OPERATIVOS DOCUMENTADOS.

ARTÍCULO 41.- Se debe contar con procedimientos operativos documentados, autorizados y comunicados a todos los usuarios que los necesiten. Los procedimientos deben incluir los procesos a ejecutar, los

controles a realizar, la modalidad de registración de las actividades tanto satisfactorias como fallidas y los mecanismos de escalamiento de problemas.

GESTIÓN DE LA CAPACIDAD.

ARTÍCULO 42.- Previa consideración de la criticidad de los activos informáticos, se debe desarrollar un informe de análisis de capacidad de los activos más importantes, y luego efectuar un monitoreo periódico para evaluar el grado de cumplimiento del citado informe.

CONTROLES CONTRA CÓDIGO MALICIOSO.

ARTÍCULO 43.- Se deben implementar mecanismos de protección contra código malicioso para prevenir, detectar, responder, contener y recuperarse rápidamente de cualquier incidente. Se debe restringir la instalación de software no autorizado y promover actividades periódicas de capacitación para las áreas técnicas y de concientización a los usuarios. Se deben controlar los archivos intercambiados a través del correo electrónico o cualquier otro medio. Los controles deberán implementarse en todos los ambientes de procesamiento y en las copias de resguardo; y deberá prestarse especial atención a las soluciones de alta disponibilidad que, si bien contribuyen a la recuperación de las operaciones en caso de contingencia, también se convierten en un medio de propagación de software malicioso y/o datos dañados. Las herramientas utilizadas para detectar y eliminar código malicioso deben mantenerse actualizadas contra nuevas amenazas. En caso de contagio deben mantenerse informadas todas las partes interesadas, tal como se determina en la Sección XIII.

RESGUARDO DE LA INFORMACIÓN.

ARTÍCULO 44.- Debe desarrollarse una estrategia de resguardo y recuperación de información que permita hacer frente a los requisitos de disponibilidad de la misma, considerando las necesidades del negocio y las disposiciones legales, reglamentarias y/o contractuales aplicables. Se debe contar con procedimientos formalmente documentados, autorizados y comunicados que describan los aspectos salientes de dicha estrategia. Se deben definir claramente las responsabilidades de los involucrados, tanto de los propietarios de los datos como de las áreas técnicas.

ARTÍCULO 45.- Deben resguardarse datos, programas, sistemas operativos y todo activo de información que se considere relevante. La organización debe mantener inventarios permanentemente actualizados de los resguardos y demás registros de utilidad para su control y eventual restauración.

ARTÍCULO 46.- A partir de un análisis de riesgo, se deben determinar las estrategias y las prioridades de resguardo, el tipo de soporte a utilizar (por ejemplo: resguardo en medios de almacenamiento magnéticos/ ópticos, esquemas de alta disponibilidad con redundancia de datos, etc.), la cantidad de copias a mantener, la ubicación física de los resguardos (se deberá demostrar que la ubicación del servicio de contingencia o resguardo de la información no será alcanzado por los mismos riesgos en forma simultánea), los períodos de retención, y la frecuencia y modalidad de las pruebas de restauración. Las copias de resguardo de los datos deben contar con medidas de seguridad equivalentes a las de los datos originales. El período de retención no podrá ser inferior a lo requerido por legislación y reglamentación vigente. Al menos se deberá contar con un juego de resguardos fuera del lugar donde la CMI procesa la información.

REGISTRO DE EVENTOS.

ARTÍCULO 47.- Se deben producir, conservar y revisar periódicamente los registros de eventos en los cuales se registren las actividades de los usuarios, las excepciones, los errores y los eventos de seguridad de la información, prestando especial atención al registro y revisión de las actividades ejecutadas por los titulares de las cuentas de usuarios privilegiados, usuarios de emergencia y con accesos especiales.

ARTÍCULO 48.- A partir de los registros de eventos, se deben conducir investigaciones forenses de incidentes cibernéticos y producir información de utilidad para el esclarecimiento de los hechos y la

prevención de ataques futuros.

PROTECCIÓN DE LA INFORMACIÓN DE LOS REGISTROS.

ARTÍCULO 49.- Los registros de eventos deben ser protegidos contra accesos no autorizados, borrado y manipulación. Deben contar con una estrategia de resguardo que los preserve en caso de contingencia y garantice su disponibilidad durante los plazos exigibles.

CONTROL DE LAS VULNERABILIDADES TÉCNICAS.

ARTÍCULO 50.- Se deben conocer las vulnerabilidades técnicas de los activos informáticos, evaluar la exposición a las vulnerabilidades y tomar las medidas apropiadas para mitigar los riesgos asociados. Partiendo de un inventario completo y actualizado de los activos, se deben implementar mecanismos eficaces de gestión de las vulnerabilidades de seguridad con el objetivo de prevenir su explotación externa y/o interna. Para la detección temprana de las vulnerabilidades se pueden emplear diferentes técnicas como por ejemplo los test de intrusión que, simulando un ataque real, ayudan a identificar vulnerabilidades en las redes, los sistemas, los procesos o en el comportamiento de las personas.

ARTÍCULO 51.- Una vez identificadas vulnerabilidades de seguridad que afecten los sistemas y que puedan estar siendo explotadas, deben probarse y aplicarse los parches críticos, o tomar otras medidas de protección, tan rápida y extensamente como sea posible. Se debe establecer un proceso para priorizar y solucionar los problemas identificados y realizar una validación posterior para evaluar si se han abordado completamente las brechas de seguridad.

SECCIÓN VIII

GESTIÓN DE COMUNICACIONES.

GESTIÓN DE LA SEGURIDAD DE LA RED.

ARTÍCULO 52.- Se debe asegurar la protección de la información crítica en las redes y sus instalaciones de procesamiento de información.

52.1. CONTROLES DE RED.

Se deben implementar controles para garantizar la seguridad de la información en las redes y la protección de los servicios conectados contra el acceso no autorizado.

52.2. SEGURIDAD DE LOS SERVICIOS DE RED.

Los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de los servicios de red deben identificarse y ser formalizados en acuerdos de servicios.

Se deben contemplar los servicios provistos desde redes internas, que son consumidos por usuarios internos y externos.

52.3. SEGREGACIÓN EN REDES.

Los grupos de servicios, usuarios y sistemas de información crítica deben ser segregados en redes. El acceso entre redes está permitido, pero debe ser controlado en el perímetro. Los criterios para la segregación de redes y el acceso permitido deben basarse en una evaluación de los requisitos de seguridad de acceso a la información crítica.

SECCIÓN IX

GESTIÓN DE PLATAFORMAS PRODUCTIVAS.

GENERALIDADES.

ARTÍCULO 53.- Se debe contar con procedimientos documentados y comunicados de gestión del cambio en la infraestructura, software de base y aplicaciones, que regulen el proceso de cambio o instalación de nuevos elementos desde los entornos de desarrollo hasta la puesta en producción. Se deben asignar claras responsabilidades para todos los intervinientes en el proceso y se contará con mecanismos de registro y control de los cambios efectuados.

ARTÍCULO 54.- Las modificaciones deben realizarse a partir de una justificación técnica o de negocio válida y deben contar con su respectiva autorización. Cualquier cambio debe considerar la evaluación de los impactos potenciales, incluyendo los impactos en la seguridad de la información y los riesgos cibernéticos.

ARTÍCULO 55.- Tanto para el desarrollo de nuevos aplicativos como para el mantenimiento de los existentes, debe definirse el ciclo de vida del proceso de desarrollo considerando aspectos como la separación de ambientes; la segregación de funciones entre los distintos responsables del proceso; el estricto control de versiones de programas y de la correspondencia entre los programas fuente y los ejecutables. Los procedimientos deben contemplar pruebas, controles y validaciones tanto para los desarrollos propios como para los tercerizados.

ARTÍCULO 56.- Se debe disponer de procedimientos planificados de vuelta atrás para la recuperación de la situación ante situaciones imprevistas o cambios que resulten fallidos.

ARTÍCULO 57.- Se debe contar con procedimientos de cambio de emergencia para permitir la aplicación rápida y controlada de los cambios necesarios para resolver un incidente. En estos procedimientos se debe detallar el mecanismo de obtención y modificación del código fuente, y los controles detectivos a realizar con posterioridad al cambio por parte de personal independiente.

GESTIÓN DE REQUERIMIENTOS Y REQUISITOS DE SEGURIDAD/CONTROLES.

ARTÍCULO 58.- Los requisitos legales, reglamentarios, contractuales y de negocio deben contemplarse desde el inicio de las tareas de adquisición, desarrollo o mantenimiento de los sistemas de información, considerando los riesgos inherentes y las necesidades de protección de los activos de información, incluyendo su integridad, disponibilidad y confidencialidad.

ARTÍCULO 59.- Los requerimientos de seguridad deben evaluarse desde la misma fase de diseño, ya que la incorporación temprana de medidas de seguridad y controles en las aplicaciones, reduce el riesgo de introducción involuntaria o malintencionada de vulnerabilidades en el entorno productivo.

Los aspectos relativos a la ciberseguridad deben también considerarse en etapas tempranas del desarrollo de los sistemas, aplicando medidas de protección contra las amenazas más frecuentes y diseñando controles detectivos y correctivos que faciliten la respuesta a incidentes y permitan restablecer las operaciones críticas en caso de ataque, preservando la integridad de las transacciones y los datos.

Dado el carácter interconectado del mercado de capitales, deben establecerse oportunamente los requisitos de resiliencia frente a ciberataques, que aseguren la disponibilidad de las interconexiones necesarias para la prestación de los servicios críticos.

ARTÍCULO 60.- En cuanto a los requerimientos funcionales de los aplicativos nuevos o modificados, se deberán adoptar las mejores prácticas en materia de control interno, incorporando desde el inicio validaciones y controles automatizados que reduzcan hasta un nivel aceptable para el negocio los riesgos de errores, duplicaciones, faltantes o alteraciones en el ingreso, procesamiento, transmisión, almacenamiento y conciliación de los datos.

ARTÍCULO 61.- Debe existir una clara y documentada vinculación entre las nuevas versiones de los elementos desarrollados y los requerimientos que le dieron origen.

ARTÍCULO 62.- Cuando las aplicaciones a adquirir o desarrollar trascienden los límites de las redes locales y atraviesen redes públicas, se deben tomar medidas adicionales de protección acordes con el nivel de los riesgos identificados y documentados. Entre los controles a considerar, se valorará el cifrado de la información transmitida; la implementación de métodos de autenticación seguros; la utilización de tecnologías que garanticen la integridad, confidencialidad y no repudio de la información compartida (por ejemplo, a través del uso de criptografía de clave pública y firmas digitales).

ARTÍCULO 63.- Se deben establecer los acuerdos de nivel de servicio entre los participantes, especialmente en lo referido a la autorización de las transacciones que atraviesan redes públicas con el objetivo de minimizar el riesgo de litigios entre las partes.

DESARROLLO SEGURO.

ARTÍCULO 64.- Deben incorporarse prácticas de codificación segura que resulten pertinentes a la infraestructura tecnológica utilizada, debiendo mantenerse las mismas actualizadas para incluir oportunamente medidas que mitiguen las nuevas amenazas. Los desarrolladores y los testers deben recibir capacitación continua sobre las vulnerabilidades conocidas a cada momento y sobre las prácticas de codificación segura que la industria vaya publicando y promoviendo (por ejemplo: OWASP Guide, Cert Secure Coding Standard, etc.).

Estas prácticas aplican tanto para las tareas de desarrollo internas como para las realizadas por terceros.

SEPARACIÓN DE ENTORNOS DE DESARROLLO, PRUEBA Y PRODUCCIÓN.

ARTÍCULO 65.- Se deben separar los entornos de producción de los de desarrollo y pruebas, de forma tal que los productivos sean totalmente independientes de los restantes; promoviendo una adecuada segregación de funciones entre el personal dedicado al desarrollo/mantenimiento de los sistemas y los responsables de la operación de los mismos. Los encargados de los despliegues en el ambiente productivo deben ser independientes de las áreas a cargo del desarrollo.

Para reforzar la separación, se deben establecer controles de acceso específicos (físicos y/o lógicos) para cada ambiente, en función de las actividades a cargo de los distintos responsables del proceso (desarrolladores, testers, implementadores, administradores, operadores, usuarios, proveedores, etc.)

PRUEBAS.

ARTÍCULO 66.- Los sistemas de información nuevos y sus modificaciones, tanto para los desarrollos propios como para los productos de terceros, deben ser probados en un ambiente de prueba en forma previa a su pasaje al entorno de producción.

Las pruebas deben diseñarse para determinar que el sistema funcione como se espera y cumple con los requisitos funcionales, de integración con otros sistemas y de seguridad que dieron origen al desarrollo/mantenimiento. La naturaleza y alcance de las pruebas debe quedar documentado en base a la evaluación realizada por el área de desarrollo y el usuario aprobador del requerimiento. Se valorará que las pruebas consideren aspectos tales como funcionalidad, usabilidad, integración con otras piezas de software y ciberseguridad.

ARTÍCULO 67.- Las pruebas deben realizarse en entornos destinados a tal fin y que representen razonablemente los entornos productivos. Deben tomarse los recaudos para evitar que los datos personales y/o confidenciales (tanto datos maestros como información que agregada resulte crítica) sean utilizados en ambientes distintos al entorno de producción.

Si fuera necesario utilizar información personal o de carácter confidencial para propósitos de prueba, todos los datos sensibles deberán ser protegidos mediante su enmascaramiento u otras medidas de protección que impidan su divulgación a personal distinto al estrictamente autorizado en los ambientes productivos.

ARTÍCULO 68.- Las pruebas, especialmente las que abarcan los aspectos de ciberseguridad, deben ser llevadas a cabo por personal técnico con la capacitación adecuada y actualizada.

Los propietarios de los datos deben participar en las pruebas de aceptación final, con el objetivo de validar que los sistemas cumplen con los requerimientos de negocio que motivaron el desarrollo.

PAQUETES DE SOFTWARE Y DESARROLLO TERCERIZADO.

ARTÍCULO 69.- En el caso de utilizar paquetes de software de terceros para operaciones definidas críticas para el negocio, se deben contemplar procedimientos para el acceso a los programas fuentes en caso de que el proveedor no pueda responder a las exigencias locales. En la medida de lo posible, los sistemas de terceros deben utilizarse tal como son provistos por su fabricante. Se deben definir contractualmente los derechos y obligaciones de cada parte en lo relativo al mantenimiento del sistema, tomando los recaudos contractuales pertinentes para asegurar el sostenimiento del paquete de software en caso de que el fabricante se vea imposibilitado de dar el soporte necesario.

Los cambios propuestos por el fabricante deben ser probados en un ambiente de prueba y homologados por la organización en forma previa a su implementación.

ARTÍCULO 70.- En los casos en que se decida delegar en terceros las actividades de desarrollo de los sistemas, las organizaciones mantienen la responsabilidad por el producto final, tanto en lo relativo al cumplimiento de los requisitos de negocio, contractual y legal, como en lo referido a las medidas de seguridad, controles adoptados y documentación de los aplicativos.

ARTÍCULO 71.- Las organizaciones y sus proveedores de servicios de desarrollo de software deben establecer contratos que determinen al menos:

- Los derechos de propiedad intelectual de los aplicativos.

- La propiedad del código fuente.

- Las garantías para el cumplimiento del contrato y las penalidades en caso de incumplimiento.

- Los criterios de aceptación de los entregables.

- Los requisitos de documentación.

- El derecho de la organización y de sus entes de contralor para realizar auditorías sobre los procesos de construcción/prueba de software del proveedor.

- La obligatoriedad del proveedor de software de comunicar en forma fehaciente, con al menos 3 (tres) años de anticipación, la fecha prevista de caducidad de la versión instalada y/o sus servicios de soporte.

- La obligatoriedad del proveedor/propietario del software de comunicar en forma fehaciente, con al menos 5 (cinco) años de anticipación, la decisión de discontinuar el producto, otorgando en dicha circunstancia la posibilidad de entregar a la organización los programas fuente, sin derecho de comercialización.

- La obligatoriedad del proveedor de adherir a las prácticas de desarrollo seguro, las metodologías de prueba y las medidas adoptadas en materia de ciberseguridad por la organización, sometiéndose a las revisiones y validaciones que la organización considere pertinentes para controlar el cumplimiento de lo requerido y la calidad del software.

ARTÍCULO 72.- Las organizaciones deberán monitorear las medidas de protección utilizadas por el proveedor contra las vulnerabilidades conocidas y realizar pruebas del software en forma previa a su pasaje al ambiente de producción.

SECCIÓN X

RELACIONES CON PROVEEDORES.

ARTÍCULO 73.- Un CMI podrá tercerizar el desarrollo, la homologación, el procesamiento y la explotación de la totalidad o una parte de sus plataformas productivas, como así también la totalidad o parte de la infraestructura principal o de contingencia. La estrategia de tercerización de la CMI deberá estar contemplada en el marco de resiliencia de seguridad, de manera tal que los riesgos derivados de dicha tercerización se encuentren en los niveles aceptados por la Dirección. El CMI deberá solicitar al proveedor del servicio un informe de cumplimiento sobre lo requerido por el presente documento por parte de un profesional independiente, tales como ISAE del tipo II o SOC del tipo II, o permitir el acceso del auditor de la CMI para una revisión in situ.

SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES.

ARTÍCULO 74.- Se deben asegurar aquellos activos de la organización que son accedidos por proveedores y externos. Es de suma importancia que todos los participantes comprendan los objetivos de recuperación y que puedan tomar acciones preventivas, ya que un incidente puede afectar a todo el ecosistema.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES.

ARTÍCULO 75.- Se deben acordar con los proveedores y formalizar los requisitos relativos a la seguridad de la información, detallando los posibles riesgos y sus respectivas medidas mitigantes.

TRATAMIENTO DE LA SEGURIDAD EN LOS ACUERDOS CON LOS PROVEEDORES.

ARTÍCULO 76.- Acuerdos de confidencialidad. Se deben formalizar las condiciones y obligaciones de parte de los proveedores en relación al tratamiento de la información de los clientes. Los acuerdos deben detallar los métodos de recuperación en caso de que un incidente comprometa la confidencialidad o integridad, para asegurar que la información pueda ser recuperada en tiempo y forma, acorde a los plazos definidos. En caso de transmitir, procesar o almacenar por medios lógicos o físicos compartidos con terceros, el proveedor deberá demostrar las medidas aplicadas para asegurar la confidencialidad de la información.

CADENA DE SUMINISTRO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

ARTÍCULO 77.- Los acuerdos con los proveedores deben incluir requisitos para tratar los riesgos asociados al suministro de tecnologías y comunicaciones, considerando (pero no limitándose) a los procesos de otros mercados, cámaras compensadoras, proveedores de energía, etc.

ARTÍCULO 78.- Se debe solicitar que cada participante establezca su tiempo de recuperación ante incidentes, para poder medir el impacto en la propia infraestructura.

Si los tiempos de recuperación fueran mayores a los propios, se deben establecer medidas mitigantes o exigir al participante que establezca un tiempo -como mínimo- igual o menor al de la propia organización.

Los acuerdos deben asegurar que todos los interesados puedan tener acceso a la información necesaria para tratar el riesgo de cada participante.

GESTIÓN DE LA ENTREGA DE SERVICIOS PRESTADOS POR LOS PROVEEDORES.

ARTÍCULO 79.- Las CMI deben asegurarse que la prestación de servicios de los proveedores que resulten críticos se realice en los términos y condiciones pactados.

La revisión de los servicios de los proveedores debe asegurar que se respeten y mantengan vigentes los términos y condiciones de los acuerdos asumidos a lo largo de la contratación. Para lo cual se debe requerir la documentación actualizada solicitada al momento de la contratación y si se necesitara adquirir nuevos servicios para una nueva funcionalidad, documentación que compruebe la capacidad del proveedor para dar dicho servicio.

SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS PRESTADOS POR LOS PROVEEDORES.

ARTÍCULO 80.- Las CMI deben revisar y auditar periódicamente la prestación de servicios de los proveedores que resulten críticos.

Deberá solicitar al proveedor del servicio un informe de cumplimiento sobre lo requerido por el presente documento por parte de un profesional independiente, tales como ISAE del tipo II o SOC del tipo II, o permitir el acceso del auditor de la CMI para una revisión in situ.

SECCIÓN XI

MONITOREO.

ARTÍCULO 81.- La Dirección debe promover un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre debilidades, eventos de seguridad y su temprana detección; manteniendo una actividad proactiva mediante un adecuado monitoreo de las condiciones de seguridad que permitan montar contramedidas oportunas y apropiadas ante los incidentes.

RESPONSABILIDADES Y PROCEDIMIENTOS.

ARTÍCULO 82.- Se deben establecer las responsabilidades y los procedimientos para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

PRESENTACIÓN DE INFORMES SOBRE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN.

ARTÍCULO 83.- Los eventos de seguridad de la información se deben informar a través de los canales apropiados, tan pronto como sea posible.

PRESENTACIÓN DE INFORMES SOBRE LAS VULNERABILIDADES DE SEGURIDAD DE LA INFORMACIÓN.

ARTÍCULO 84.- Se debe requerir a los empleados y contratistas usuarios de los sistemas de información de la organización, que informen cualquier vulnerabilidad de seguridad de la información observada o sospechada en sistemas o servicios. Se deben realizar análisis exhaustivos para determinar la naturaleza y extensión de los incidentes así como el daño infligido. Mientras la investigación está en curso, se deben tomar medidas inmediatas para contener la situación con el objetivo de prevenir daños adicionales y comenzar los esfuerzos de recuperación para restaurar las operaciones basadas en su planificación de respuesta.

EVALUACIÓN Y DECISIÓN SOBRE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN.

ARTÍCULO 85.- Se deben evaluar los eventos de seguridad de la información y decidir si se los debe clasificar como incidentes de seguridad de la información y asegurar la recolección de información para el proceso de investigación forense.

RESPUESTA A LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

ARTÍCULO 86.- Se debe responder a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

Al registrar los incidentes, se deben documentar como mínimo:

● Equipo, usuario, servicio o aplicación afectada

● Ubicación física, horario y día

● Síntomas detectados

● Acciones realizadas

● Cualquier otra información que se considere de relevancia

APRENDIZAJE A PARTIR DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

ARTÍCULO 87.- Se debe utilizar el conocimiento obtenido del análisis y resolución de los incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros. Debe asegurarse de que todo el personal, ya sea permanente o temporal, reciba capacitación para desarrollar y mantener una conciencia apropiada y las competencias necesarias para detectar y abordar los riesgos de seguridad.

RECOLECCIÓN DE LA EVIDENCIA.

ARTÍCULO 88.- La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la información que se pueda utilizar como evidencia y debe tener la capacidad de asistir o llevar a cabo investigaciones forenses de incidentes cibernéticos y establecer políticas de registro relevantes que incluyan los tipos de evidencias que se deben mantener y sus períodos de retención.

SECCIÓN XII

GESTIÓN DE CONTINUIDAD DEL NEGOCIO.

GESTIÓN DE LA CONTINUIDAD.

ARTÍCULO 89.- Se debe incorporar la continuidad del negocio como parte de los sistemas de gestión de la organización.

El Directorio/Comité es el responsable de aprobar la identificación, la valorización, la gestión y el control de los riesgos relacionados con la continuidad del negocio. Debe asegurar la existencia y la provisión de los recursos necesarios para la creación, mantenimiento y prueba de un plan de recuperación del procesamiento de información automática.

La CMI debe asegurarse de que:

a) Se defina una estructura de gestión del Plan de Continuidad del Negocio acorde con el detalle de sus funciones y responsabilidades relacionadas con esta gestión.

b) Se identificarán las diferentes tipologías de incidentes que alcanzará a la infraestructura de la CMI.

c) Se identifique el personal de respuesta a incidentes con la responsabilidad necesaria, autoridad y competencia para gestionar un incidente y mantener la seguridad de la información;

d) los planes de procedimientos documentados, respuesta y recuperación sean desarrollados y aprobados, que detallen cómo la organización gestionará un evento perjudicial y mantendrá su seguridad de la información a un nivel predeterminado.

De acuerdo con los requisitos de continuidad seguridad de la información, la organización debe establecer, documentar, implementar y mantener controles de seguridad de la información dentro de los procesos de continuidad de negocio o de recuperación de desastres.

Se deben identificar toda la legislación aplicable a su organización con el fin de cumplir con los requisitos para la CMI.

PLANIFICACIÓN DE LA CONTINUIDAD DEL NEGOCIO.

ARTÍCULO 90.- La continuidad del procesamiento de datos automático, que en definitiva posibilita la continuidad de los negocios, deberá evidenciar que se han identificado los eventos que puedan ocasionar interrupciones en sus procesos críticos.

Es responsabilidad del Comité/Directorio aprobar la evaluación de riesgos para determinar el impacto de distintos eventos, tanto en términos de magnitud de daño como del período de recuperación y la vuelta a la normalidad.

Estas actividades deben llevarse a cabo con la activa participación de los propietarios de los procesos y recursos de negocio. La evaluación considerará todos los procesos de negocio alcanzados por esta norma y no se limitará sólo a las instalaciones de procesamiento de la información, sino también a todos los recursos relacionados.

Los resultados de la evaluación deben ser el soporte para la selección de mecanismos alternativos de recuperación y adopción de medidas preventivas para la confección del plan de recuperación y vuelta a la normalidad del procesamiento de datos.

IMPLEMENTACIÓN DE PLAN DE CONTINGENCIA.

ARTÍCULO 91.- Las instalaciones alternativas de procesamiento de datos deben atender los requisitos mínimos establecidos por estas normas, pudiendo ser propias o de terceros.

El equipamiento de las instalaciones de procesamiento alternativo debe contemplar la capacidad de administración y gestión de todos los procesos de negocios clasificados como críticos para asegurar mantener la actividad mínima definida por la CMI.

La instalación alternativa debe prever la existencia de equipamiento destinado a las telecomunicaciones para acceder al servicio mínimo que brinda.

En caso de un siniestro o suceso contingente que torne inoperantes las instalaciones principales, la localización de las instalaciones alternativas deberá ser tal que no sean alcanzadas por el mismo evento. Además, deberán tornarse totalmente operacionales en condiciones idénticas, en una ventana de tiempo tal que no afecte la operación.

La selección de la localización antes mencionada deberá estar soportada por la evidencia documental de la existencia de un análisis de riesgo de eventos simultáneos, que están fehacientemente expresados en el mismo.

IMPLEMENTACIÓN DE LA CONTINUIDAD DEL NEGOCIO.

ARTÍCULO 92 - Se debe evidenciar la existencia de un procedimiento escrito, aprobado formalmente, para atender a la continuidad del procesamiento actividades vinculadas, en el caso que se presenten

contingencias o emergencias.

El documento deberá basarse en el mismo análisis de riesgo efectuado para determinar la localización de las instalaciones alternativas de procesamiento de datos, enunciando todos los posibles escenarios que harían que el plan entrará en funcionamiento.

El mismo deberá, como mínimo, contener lo siguiente:

• Procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente. Estos deben incluir disposiciones con respecto a la gestión de vínculos eficaces a establecer con las autoridades públicas pertinentes, por ej.: entes reguladores, policía, bomberos y otras autoridades.

• Los datos de contacto del personal clave.

• Las aplicaciones críticas y su prioridad con respecto a los tiempos de recuperación y regreso a la operación normal.

• El detalle de los proveedores de servicios involucrados en las acciones de contingencia / emergencia.

• La información logística de la localización de recursos claves, incluyendo: ubicación de las instalaciones alternativas, de los resguardos de datos, de los sistemas operativos, de las aplicaciones, los archivos de datos, los manuales de operación y documentación de programas / sistemas / usuarios.

PRUEBA DEL PLAN DE CONTINUIDAD.

ARTÍCULO 93.- El plan de continuidad de procesamiento de datos debe ser probado periódicamente, como mínimo una vez al año. Las pruebas deben permitir asegurar la operatoria integral de todos los sistemas automatizados críticos a efectos de verificar que el plan está actualizado y es eficaz. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente del plan mencionado.

Deberá evidenciarse la existencia de un cronograma formal de pruebas que indicará cómo debe probarse cada elemento del plan, y la fecha en la cual cada una de las pruebas deberá ser efectuada.

En las pruebas deben participar las áreas usuarias de los procesos de negocio, quienes deben verificar los resultados de las mismas. Se deberá documentar formalmente su satisfacción con el resultado de la prueba como medio para asegurar la continuidad de los procesos de negocio en caso de que ocurra una contingencia. La auditoría interna de la entidad también deberá conformar la satisfacción por el resultado de las mismas a tal efecto.

El informe realizado por las áreas usuarias y de auditoría interna deberá ser tomado en conocimiento por el Comité/Directorio.

VERIFICACIÓN, REVISIÓN Y VALORACIÓN DE LA CONTINUIDAD DEL NEGOCIO.

ARTÍCULO 94.- Los cambios organizativos, técnicos, de procedimiento y de procesos, ya sea en un contexto operacional o de continuidad, pueden conducir a cambios en los requisitos de continuidad seguridad de la información. En tales casos, la continuidad de los procesos, procedimientos y controles para la seguridad de la información debe ser revisada en contra de estos requisitos que han cambiado.

Las organizaciones deben verificar su información de gestión de la continuidad para la revisión de la validez y eficacia de las medidas de continuidad de seguridad de la información, cuando los sistemas de información, procesos de seguridad de la información, procedimientos y controles o procedimientos de gestión de recuperación de gestión / desastre de continuidad de negocio y soluciones cambian.

REDUNDANCIAS.

ARTÍCULO 95.- Las organizaciones deben identificar los requisitos para la disponibilidad de los sistemas de información. Cuando la disponibilidad no puede ser garantizada mediante la arquitectura de los sistemas existentes, componentes o arquitecturas redundantes deben ser considerados.

Los sistemas de información redundantes deben ser probados para asegurar la conmutación por error de un componente a otro según lo previsto.

SECCIÓN XIII

RELACIÓN CON OTRAS PARTES INTERESADAS.

ECOSISTEMA.

ARTÍCULO 96.- Las partes interesadas (mercados, proveedores de servicio y cualquier otra organización asociada) conforman un ecosistema, con sistemas interconectados y objetivos en común. Con esta premisa, los objetivos de negocio de cada una de las partes deben estar alineados a poder cumplir con los tiempos de recuperación establecidos para el ecosistema en conjunto.

CANAL DE CONTACTO.

ARTÍCULO 97.- Las partes interesadas deben definir un canal de contacto que permita comunicar de forma fehaciente e inmediata cualquier mensaje que las mismas consideren de relevancia.

DOCUMENTACIÓN DE INTERCONEXIONES.

ARTÍCULO 98.- Las partes interesadas deben identificar e inventariar todos los componentes, servicios y sistemas asociados a la plataforma de interconexión. Este inventario debe ser revisado y actualizado al menos una vez por año, o cada vez que la organización lo considere necesario.

IDENTIFICACIÓN DE RIESGOS.

ARTÍCULO 99.- Las partes interesadas deben identificar los riesgos inherentes asociados a cada uno de los componentes que componen el inventario mencionado en el artículo anterior, o que puedan derivar de incidentes ocurridos en plataformas externas.

PRUEBAS CONJUNTAS.

ARTÍCULO 100.- Se deben realizar pruebas en conjunto, y si existiera conflicto de intereses, el ente regulador debe intervenir para arbitrar, supervisar o dar consistencia a los objetivos buscados.

AMBIENTE DE PRUEBAS.

ARTÍCULO 101.- Las partes interesadas deberán tener disponibles ambientes de pruebas funcionalmente equivalentes a los ambientes productivos, que permitan validar el correcto funcionamiento de eventuales cambios en forma previa a la puesta en producción de los mismos.

CONTROL DE CAMBIOS.

ARTÍCULO 102.- En caso de que se planifique o detecte un cambio en las plataformas y servicios de uso compartido o asociadas a la interconexión, la organización responsable debe enviar un aviso a todo el ecosistema en tiempo y forma, a fin de permitirle al resto de las entidades realizar las adecuaciones y pruebas necesarias, utilizando el canal de contacto definido.

ACUERDOS DE INTERCAMBIO DE INFORMACIÓN.

ARTÍCULO 103.- Todo sistema o servicio que represente una plataforma de interconexión debe estar respaldado por un acuerdo de intercambio de información que contemple las acciones a tomar en caso de incidentes que atenten contra la confidencialidad, integridad o disponibilidad de la información afectada.

DETECCIÓN DE VULNERABILIDADES.

ARTÍCULO 104.- En el caso de que alguna de las partes interesadas detecte una amenaza o situación que pueda afectar a la integridad, disponibilidad o confidencialidad de la información en la plataforma de interconexión, deberá dar un aviso al ente regulador, utilizando el canal de contacto establecido anteriormente.

RESPUESTAS ANTE INCIDENTES.

ARTÍCULO 105.- En caso de ocurrencia de incidentes, las partes interesadas involucradas deben colaborar solidariamente brindando información que pueda servir para tareas forenses.

SINCRONIZACIÓN DE RELOJES.

ARTÍCULO 106.- Se debe definir un servicio de sincronización de relojes, utilizando servidores NTP reconocidos en el mercado, a fin de lograr la sincronización exacta de todos tiempos y relojes críticos utilizados para la interconexión".

ARTÍCULO 3°.- La presente Resolución General entrará en vigencia a partir del día siguiente al de su publicación en el Boletín Oficial de la República Argentina.

ARTÍCULO 4°.- Regístrese, comuníquese, publíquese, dese a la Dirección Nacional del Registro Oficial, incorpórese al sitio web del Organismo en www.cnv.gob.ar, agréguese al texto de las NORMAS (N.T. 2013 y mod.) y archívese.

Digitally signed by BOEDO Patricia Noemi
Date: 2017.08.24 14:29:06 ART
Location: Ciudad Autónoma de Buenos Aires

Patricia Noemi Boedo
Vicepresidenta
Directorio
Comisión Nacional de Valores

Digitally signed by HOURBEIGT Carlos Martin
Date: 2017.08.24 15:11:22 ART
Location: Ciudad Autónoma de Buenos Aires

Carlos Martin Hourbeigt
Director
Directorio
Comisión Nacional de Valores

Digitally signed by GAVITO Martin José
Date: 2017.08.24 16:11:53 ART
Location: Ciudad Autónoma de Buenos Aires

Martin Jose Gavito
Director
Directorio
Comisión Nacional de Valores

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=MINISTERIO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2017.08.24 16:12:02 -03'00'