Políticas

9.1. Roles y Responsabilidades

9.1.1. **Definición de Incidente** – Un incidente es un evento que provoca cierto nivel de crisis y requiere llevar a cabo una acción para reducir o eliminar el riesgo causado. Puede ir desde la Intrusión a una Computadora, la Negación de Servicios (DoS), Infecciones de Virus, Acceso no autorizado, hasta eventos que normalmente llevan a tomar medidas de Recuperación ante Desastres (Disaster Recovery) como cortes de energía o desastres naturales.

9.1.2. **Grupo de Respuesta a Incidentes** – El Grupo de Respuesta a Incidentes (GRI) de la A.N.V. deberá estar formado por el Oficial de Seguridad y el Equipo de Seguridad de Información, los integrantes de Mesa de Ayuda, los Administradores de Sistemas, los Administradores de Red y la Gerencia de Sistemas. Adicionalmente se sumará personal no técnico (RRHH, Legal, Relaciones Externas), o técnico (Administradores de Bases de Datos, Desarrollo), de acuerdo al tipo de Incidente.

9.1.3. **Funciones del GRI** – Recibir los reportes de incidentes generados en la empresa, determinar su grado de importancia, escalar el problema cuando sea pertinente y tomar las acciones correctivas necesarias. Este grupo deberá entrar en acción solamente en caso de un Incidente, continuando sus miembros sus actividades habituales cuando no sea requerida su participación. También será su función la de crear, mantener y actualizar los procedimientos y guías asociados con la Respuesta a Incidentes.

9.1.4. **Líder del GRI** – El GRI deberá tener un líder, en general el Oficial de Seguridad, que será responsable por las acciones tomadas por el grupo durante el transcurso de un incidente y de coordinar dichas acciones basándose en los procesos y guías generados.

9.1.5. **Líder del Incidente** – Cada incidente deberá tener un líder "ad hoc" nombrado por el Oficial de Seguridad que será el responsable de llevar a cabo todas las actividades durante un incidente determinado. Todas las comunicaciones relativas a los progresos del incidente deberán pasar por el Líder del Incidente.

9.2. Reporte de Incidentes

9.2.1. **Datos Requeridos –** Cuando un usuario de la A.N.V. reporte un incidente a Mesa de Ayuda, deberá especificar: Fecha y Hora del reporte, quien realiza el reporte del incidente, naturaleza del mismo, cuando ocurrió, el hardware y el software involucrado.

9.3. Respuesta a Incidentes

9.3.1. **Detección Inicial** – Cuando un usuario sospeche la existencia de un incidente de seguridad, deberá reportarlo a Mesa de Ayuda, quien lo derivará al equipo de seguridad informática. Este equipo verificará su ocurrencia, los sistemas comprometidos, usuarios involucrados y su impacto potencial sobre el negocio.

9.3.2. **Estrategia de Respuesta** – Una vez determinada la ocurrencia de un incidente, el GRI deberá establecer la mejor estrategia de respuesta. Esta deberá considerar factores técnicos y del negocio y según la gravedad del mismo deberá ser aprobada por la dirección de la A.N.V.,

por lo que deberá presentarse en términos no técnicos indicando los pros y contras. Por ejemplo, Tiempo de caída de la red, Tiempo de no-acceso de usuarios al sistema, Obligaciones Legales, Imagen Pública, Robo de Propiedad Intelectual, etc.

9.4. Investigación

9.4.1. **Investigación –** Luego de aprobada la estrategia, el GRI deberá determinar el por qué, el qué, el cuándo, el dónde y cómo aislar el incidente.

9.4.2. **Procedimiento de Respuesta –** Para llevar a cabo la investigación forense del incidente, el GRI deberá construir un proceso de respuesta al incidente y una política que lo soporte. A pesar que algunas de las Políticas en las cuales se basará el proceso de respuesta son las Políticas de Seguridad actualmente aprobadas, el GRI podrá necesitar rever la forma que dichas políticas se pueden aplicar en el incidente actual y recomendar cambios que soporten las actividades en la respuesta al incidente.

9.4.3. **Recolección de Evidencias –** Durante la fase de Investigación, se deberán recabar evidencias que puedan servir para determinar y probar quién llevó a cabo el ataque y qué vulnerabilidades o errores en la configuración de los Sistemas fueron explotadas. La toma de evidencia se puede realizar durante el desarrollo del ataque.

9.5. Medidas Preventivas

9.5.1. **Implementación de Medidas de Seguridad** – La meta de esta fase será la implementación de medidas que prevengan que el incidente siga causando daño.

9.5.2. **Aislamiento del Problema** – Se deberá aislar y contener el problema que generó el incidente antes de comenzar con la recuperación de los Sistemas.

9.6. Aprendizaje

9.6.1. **Investigación Forense** –Antes de cerrar el incidente, si se justifica por su gravedad, se deberá realizar una investigación donde se estudie información recabada en las fases de Investigación y Solución para intercambiar experiencias y actualizar los procedimientos, basado en los nuevos conocimientos adquiridos. Esta investigación deberá llevarse a cabo por el Grupo de Respuesta a Incidentes, el Líder del Incidente y el Oficial de Seguridad, con la supervisión del Equipo de Seguridad de la Información, y de ser necesario, el Comité de Seguridad.

9.6.2. **Base de Conocimiento** – Los resultados de las investigaciones y las medidas correctivas tomadas en la solución de los incidentes, deberá integrar una Base de Conocimiento. Esta Base será consultada ante nuevos incidentes para determinar si los procedimientos y soluciones utilizadas son aplicables o puedan servir para generar nuevos procedimientos y soluciones.

Capítulo 10. Gestión de la Continuidad de las actividades de la A.N.V.

Introducción

La Gestión de la continuidad del negocio es un proceso crítico que debe involucrar a todos los niveles del Organismo.
La responsabilidad de la gestión de la continuidad del negocio recae en la dirección de la organización, quien deberá tener en cuenta su cometido.
El desarrollo e implementación de un sistema de gestión de la continuidad del negocio, es una herramienta básica para garantizar que las actividades de la A.N.V. se restablezcan dentro de los plazos requeridos.
Se deberá contar con un proceso formal y documentado para garantizar la continuidad del negocio, donde la capacidad de continuar las actividades sea primordial para la organización en sí, así como para sus clientes y partes interesadas.
Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y de gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades y asegurar la reanudación oportuna de las operaciones indispensables.

Objetivo – Generar los Procedimientos necesarios para minimizar los efectos de las posibles interrupciones de las actividades normales de la A.N.V. (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos del negocio mediante una combinación de controles preventivos y acciones de recuperación.
Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

a) Prevención, prueba y mantenimiento del plan.
b) Activación y Administración de la Crisis.
c) Recuperación.
d) Operación en régimen de contingencia.
e) Vuelta a la normalidad.

Incumplimiento de la Política de Seguridad de la Información

El incumplimiento de estos y otros requisitos de Seguridad de la Información puede resultar en una acción disciplinaria. En alguna ocasión, una solicitud de incumplimiento puede ser establecida, en esos casos, el incumplimiento debe ser aprobado luego de un proceso de valoración y aceptación del riesgo. El proceso requiere un memo de aceptación del riesgo firmado por los Directores y aprobado por el Equipo de Seguridad de la Información. Más detalles sobre el proceso de aceptación del riesgo pueden ser obtenidos a través de una Auditoría interna.

Preguntas sobre este documento podrán ser realizadas al Comité de Seguridad de la Información a través de correo electrónico **SEGINFO@ANV.GUB.UY**

Glosario de términos técnicos

Ad Hoc	Ad hoc es una locución latina que significa literalmente «para esto». Generalmente se refiere a una solución elaborada específicamente para un problema o fin preciso y, por tanto, no es generalizable ni utilizable para otros propósitos. Se usa pues para referirse a algo que es adecuado sólo para un determinado fin.
Autenticación	Verificación de la identidad de un usuario
Autoridad certificadora	En criptografía una autoridad de certificación, certificadora o certificante (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública
Certificado digital	Un certificado digital (también conocido como certificado de clave pública o certificado de identidad) es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad (por ejemplo: nombre, dirección y otros aspectos de identificación) y una clave pública.
Copyright	El derecho de autor es un conjunto de normas jurídicas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores (los derechos de autor), por el solo hecho de la creación de una obra literaria, artística, musical, científica o didáctica, esté publicada o inédita.
Crackers	El término cracker (del inglés crack, romper) se utiliza para referirse a las personas que rompen algún sistema de seguridad. La finalidad de los cracker es siempre el delito con beneficio económico
Detector de intrusos	Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red
Dispositivos biométricos	Dispositivos de autenticación de individuos mediante la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo
DMZ	En seguridad informática, una zona desmilitarizada (DMZ, de-militarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna.
e-Commerce	El comercio electrónico, también conocido como e-commerce (electronic commerce en inglés), consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas.
Encriptación	Criptografía (del griego krypto= «oculto», y graphos= «escribir», literalmente «escritura oculta») se ha definido como la parte de la criptología que se ocupa de las técnicas que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado y/o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes
Equipo Portátil	Se entiende por Equipo Portátil todo dispositivo móvil que proporcione portabilidad y posea capacidad de procesamiento, con conexión permanente o intermitente a la red por ejemplo: notebook, netbook, tablet, teléfonos inteligentes, etc.
Extranet	Una extranet es una red privada que utiliza protocolos de Internet, protocolos de comunicación e infraestructura pública de comunicación para compartir de forma segura parte de la información u operación propia de una organización con proveedores, compradores, socios, clientes o cualquier otro negocio u organización. Se puede decir en otras palabras que una extranet es parte de la Intranet de una organización que se extiende a usuarios fuera de ella. Usualmente utilizando Internet
Firewall	Un cortafuego (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
FTP	FTP (siglas en inglés de File Transfer Protocol, 'Protocolo de Transferencia de Archivos') en informática, es un protocolo de red para la transferencia de archivos
Hackers	Hacker (seguridad informática), una persona que irrumpe en computadoras y redes informáticas. Los hackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta o por el desafío

HTTP	Hypertext Transfer Protocol o HTTP (en español protocolo de transferencia de hipertexto) es el protocolo usado en cada transacción de la World Wide Web.
HTTPS	Hyper Text Transfer Protocol Secure (en español: Protocolo seguro de transferencia de hipertexto), más conocido por sus siglas HTTPS, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hiper Texto, es decir, es la versión segura de HTTP.
IDS	Ver Detector de intrusos
Imesh	iMesh es una aplicación de tecnología peer-to-peer que permite el intercambio de información gratuita en casi cualquier formato. Usa una red P2P (IM2Net) privada. iMesh es propiedad de la compañía americana iMesh, Inc
Información sensitiva	Toda aquella información que no es de uso público
Intranet	Una intranet es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales
ISP	Un proveedor de servicios de Internet (o ISP, por la sigla en inglés de Internet Service Provider) es una empresa que brinda conexión a Internet a sus clientes
IT	Acrónimo inglés de Information Technology (Tecnologias de la información)
KaZaa	Kazaa (antes llamado "KaZaA") es una aplicación para el intercambio de archivos entre pares
LAN	Una red de área local, red local o LAN (del inglés local area network) es la interconexión de una o varias computadoras y periféricos
Ley 18.381 art 8ª Información Secreta	Se entiende por información secreta aquella definida en ese carácter por ley.
Ley 18.381 art 9ª Información Reservada	Se clasificará como información reservada aquella cuya difusión pueda comprometer la seguridad pública o la defensa nacional; menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de reservado al Estado uruguayo; dañar la estabilidad financiera, económica o monetaria del país; poner en riesgo la vida, la dignidad humana, la seguridad o la salud de cualquier persona; suponer una pérdida de ventajas competitivas para el sujeto obligado o pueda dañar su proceso de producción; desproteger descubrimientos científicos, tecnológicos o culturales desarrollados o en poder de los sujetos obligados.
Ley 18.381 art 10ª Información Confidencial	Se clasificará como información confidencial I) la entregada en ese carácter siempre que: refiera al patrimonio de la persona; comprenda hechos o actos de carácter económico, contable, jurídico o administrativo, relativos a una persona física o jurídica, que pueda ser útil para un competidor; esté amparada por una cláusula contractual de confidencialidad y II) los datos personales que requieran previo consentimiento informado.
Logs	Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.
DNS	Domain Name System o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.
One-Time password	La autenticación con contraseña de un solo uso u OTP (del inglés One-Time Password) es una variación de la autenticación con usuario/contraseña. En este método de autenticación se dificulta el acceso no autorizado haciendo que cada contraseña sea válida para una única sesión. Se tiene que usar una contraseña nueva para cada sesión.
Peer-to-Peer	Una red peer-to-peer, red de pares, red entre iguales, red entre pares o red punto a punto (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.
Perímetro de acceso	Ver DMZ

POP3	Post Office Protocol (POP3, Protocolo de la oficina de correo) en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto
Principio Event-by-Event	Paradigma de programación en el que tanto la estructura como la ejecución de los programas van determinados por los sucesos que ocurran en el sistema, definidos por el usuario o que ellos mismos provoquen
Principio de Necesidad de conocer y usar	Asignación de privilegios mínimos necesarios para tareas especificas
Proxy	Su finalidad más habitual es la de servidor proxy, que consiste en interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos posibles como seguridad, rendimiento, anonimato, etc. Esta función de servidor proxy puede ser realizada por un programa o dispositivo
Routers	Un router —anglicismo, también conocido como encaminador, enrutador, direccionador o ruteador— es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar
SMTP	Simple Mail Transfer Protocol (SMTP) Protocolo Simple de Transferencia de Correo. Protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.)
Spam	Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor
Tecnología de dos factores	Sistema de autenticación que requiere que el usuario ingrese 2 tipos de datos para obtener acceso. El usuario tiene que validar precisamente 2 factores: algo que sabe (PIN, Password) y algo que tiene (credencial almacenada en un dispositivo de Hardware)
VPN	Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada
Web mail	Servicio de correo basado en http/https
Web server	Servidor de internet
Zona semi-segura	ver DMZ

Historia del documento

Ediciones			
Revisión	**Fecha**	**Motivo de Revisión**	**Modificaciones**
1.0	22/07/2010	Generación del Documento	Provisorio hasta revisión por parte del Comité de Seguridad de la Información.
1.1	29/12/2011	Revisión Gral. por inicio de funciones del Comité de Seguridad de la información	Se modifican definición Confidencial (4.1.1)
1.2	31/05/2012	Revisión Gral. de la política	Se cambia el punto "Requisitos previos" del Capítulo 2. Se agrega glosario de términos
1.3	01/08/2012	Revisión Gral. de la política	Se cambian varios términos del documento en general.
1.3.1	30/08/2012	Revisión Gral. de la política	Se modifica el punto 2.9.5 para que no sea muy específico acerca del adendum. Se agrega al glosario la definición de "Información sensitiva"
1.3.2	24/09/2012	Revisión Gral. de la política	Se modifica la redacción de varios puntos de la política y se modifico el capitulo 4.
1.3.3	26/10/2012	Revisión Gral. de la política	Se agrega capitulo 10.