INFORME UAIMA N° 026-001/2018

UNIDAD DE AUDITORÍA INTERNA

SECRETARÍA DE GOBIERNO DE AGROINDUSTRIA

MINISTERIO DE PRODUCCIÓN Y TRABAJO

"POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN"

Noviembre de 2018

Unidad de Auditoría Interna
Secretaría de Gobierno de Agroindustria
Ministerio de Producción y Trabajo

TABLA DE CONTENIDOS

INFORME EJECUTIVO 3
SINTESIS 3
CONCLUSIÓN 4
INFORME ANALITICO 5
I. OBJETO 5
II. ALCANCE 5
III. LIMITACION AL ALCANCE 5
IV. TAREAS REALIZADAS 5
V. MARCO DE REFERENCIA 6
VI. ACLARACIONES PREVIAS 8
VII. HALLAZGOS, IMPACTO Y RECOMENDACIONES 18
VIII. RESULTADOS OBTENIDOS DEL CUMPLIMIENTO DE OBJETIVOS ESTRATEGICOS SGN 20
IX. CONCLUSIÓN 22
ANEXO I – EVIDENCIA 24
ANEXO II – CUMPLIMIENTO DE OBJETIVOS ESTRATÉGICOS SGN 31
ANEXO III – EQUIPO DE TRABAJO 49

INFORME EJECUTIVO

SINTESIS

En virtud de las competencias otorgadas a esta Unidad de Auditoría Interna (UAI) por Decisión Administrativa N° 324/18, de fecha 15 de marzo de 2018, que abrogara la Decisión Administrativa Nº 202/11 y modificara la estructura orgánica funcional de la UAI del Ministerio de Agroindustria y en el marco de los cambios estructurales de la Administración Pública Nacional, (Decreto N° 801/18 y Decreto N° 802/18), en el cual MA adopta la denominación de Secretaría de Gobierno, dependiendo del Ministerio de Producción y Trabajo a partir del día 6 de septiembre del corriente se procedió a efectuar las tareas de relevamiento, análisis y evaluación dela Política de Seguridad de la Información imperante en el organismo.

Debe señalarse que durante las tareas propias de auditoría, las cuales se efectuaron durante los meses de junio a agosto del corriente año en las oficinas de la Unidad de Auditoría Interna, y en la Dirección de Informática (en adelante, DI) dependiente de la Subsecretaría de Coordinación Administrativa (en adelante, SCA) ocurrieron los cambios estructurales mencionados *ut supra*.

La solicitud y búsqueda de información y documentación fueron efectuadas durante los meses de junio a agosto del corriente año en las oficinas de la Unidad de Auditoría Interna, y en la Dirección de Informática (en adelante, DI) dependiente de la Subsecretaría de Coordinación Administrativa (en adelante, SCA) y ya en proceso de elaboración del informe preliminar, ocurrieron cambios de estructura en el MA que afectan este informe.

El presente informe se encuentra referido a las observaciones y conclusiones sobre el objeto de las tareas hasta la fecha precedentemente indicada y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido.

A continuación se exponen los hallazgos más significativos:

- **Inactividad del Comité de Seguridad de la Información.**
- **Falta de actualización de la lista de sistemas informáticos desarrollados que se encuentran fuera del ámbito y control de la DI.**
- **Falta de adecuación del Comité de Seguridad de la Información a la estructura vigente del MA.**
- **Falla en la depuración de permisos por cambio de área.**

CONCLUSIÓN

Las tareas se realizaron en un adecuado ambiente de control interno de acuerdo a los lineamientos impartidos por la Sindicatura General de la Nación mediante Resolución SGN Nº 152/02.

Mediante la nota NO-2018-41218154-APN-UAI#MA se remitió el presente informe para que el área auditada exponga su opinion respecto de las observaciones detalladas por esta UAI, en la cual textualmente se expresaba: "(*…) Vencido dicho plazo, y no habiéndose otorgado formalmente una prórroga al mismo, el informe se emitirá destacando la ausencia de respuesta de dicha opinión a cada observación formulada. Se adjunta el correspondiente informe para su descargo(…)"..*

Si bien a la fecha de la emision del presente informe de auditoría, no se recepciono respuesta alguna por parte del auditado, las observaciones expuestas seran objeto de revision al efectuarse las tareas de seguimiento de observaciones pendientes.

Es importante mencionar que la información es un recurso, un activo de la organización que posee valor para el Organismo, por lo que su protección a través de una adecuada Política de Seguridad Informática es necesaria a fin de mantener y preservar la seguridad del mismo.

Atento a lo expuesto y en relación a los desvíos observados, se considera necesario y de gran utilidad impulsar el Comité de Seguridad de la Información en el ámbito de la jurisdicción a fin de cumplir con los objetivos de la ONTI y la normativa vigente, Ello minimizará los riesgos y contribuirá al cumplimiento eficiente de los objetivos.

Corresponde por último señalar que las tareas de auditoría y la redacción del presente informe definitivo tuvieron lugar con anterioridad a la asunción, el día 3 de septiembre del 2018, a mí actual cargo de Auditora Interna Titular, conforme lo dispuesto por Resolución SIGEN Nº 143 de fecha 24 de agosto del corriente.

En este sentido, se hace constar que, con la limitación de responsabilidad que la situación descripta conlleva, se suscribe el presente a los fines de posibilitar la correcta ejecución de la Planificación Anual de esta Unidad de Auditoría Interna aprobada para el ejercicio 2018.

Buenos Aires, 07 de noviembre de 2018

SANTARELLI
Giselle Eliana

Firmado digitalmente por SANTARELLI Giselle Eliana
Nombre de reconocimiento (DN): serialNumber=CUIL 27266203700, c=AR, cn=SANTARELLI Giselle Eliana
Fecha: 2018.11.07 16:58:21 -03'00'

INFORME ANALITICO

I. OBJETO

El objeto del presente es analizar, verificar y corroborar el cumplimiento de la Política de Seguridad de la Información a la actual Secretaría de Gobierno[1] de Agroindustria de acuerdo a la normativa específica y vigente.

También, se aplicó el instructivo de trabajo relativo a procedimientos necesarios para abordar los objetivos estratégicos planteados por la Sindicatura General de la Nación en los Lineamientos para la Planificación del ejercicio 2018.

II. ALCANCE

Las tareas de auditoría se llevaron a cabo de acuerdo a los criterios establecidos en las Normas de Auditoría Interna Gubernamental Resolución SGN N° 152/02, Normas Generales de Control Interno Resolución SGN Nº 172/14 y, los conceptos y procedimientos estipulados en el Manual de Control Interno Gubernamental; todo ello de la Sindicatura General de la Nación.

La labor se realizó en el período comprendido entre los meses de junio y agosto de 2018 inclusive.

El análisis se realizó sobre las tareas y acciones que la Dirección de Informática (DI) dependiente de la Subsecretaría de Coordinación Administrativa (SsCA) del ex MA realizó en virtud de la seguridad informática. Así como también las Actas del Comité de Seguridad de la Información del entonces Ministerio.

III. LIMITACION AL ALCANCE

Se presenta como limitación al presente informe la falta de respuesta al punto 3 del requerimiento solicitado mediante NO-2018-27205901-APN-UAI-MA y reiterada por NO-2018-33271727-APN-UAI, sin respuesta a la fecha del presente informe por la Dirección de Informática.

IV. TAREAS REALIZADAS

Las tareas de auditoría desarrolladas fueron las siguientes:

- Análisis de la normativa vigente y su cumplimiento.
- Envío de NO-2018-26208455- APN-UAI-MA de Inicio de Auditoría.

[1] Según Decreto N° 801/18 y Decreto N° 802/18 el Ministerio de Agroindustria adopta la denominación de Secretaría de Gobierno dependiendo del Ministerio de Producción y Trabajo a partir del día 04/09/18.

- Envío de nota de Solicitud de Información NO-2018-27205901-APN-UAI-MA, a la Dirección de Informática.
- Envío de NO-2018-32908474-APN-UAI-MA remitiendo el Cuestionario Sobre Cumplimientos Estratégicos SIGEN para el año 2018.
- Análisis de la información suministrada por la Dirección de Informática, dependiente de la Subsecretaría de Coordinación Administrativa mediante NO-2018-32702521-APN-DI-MA, de fecha 10 de julio del corriente año.
- Reunión con el Director de Informática, el día 04 de julio de 2018.
- Relevamiento de la existencia de Manuales Operativos o Instructivos y análisis del grado de cumplimiento de los mismos.
- Verificar el estado de la ejecución y cumplimiento de la normativa ONTI Nº 1/2015.
- Verificación de la existencia escrita y correcta actualización de nomas de programación y tecnología.
- Análisis y verificación de la ejecución de la política de la información en el entonces Ministerio de Agroindustria
- Inspección ocular el día 3 de agosto de 2018 sobre el Proceso de Generación y Resguardo de Backups en el subsuelo de Paseo Colon Nº 922 y el Proceso de Acción de Alarma en Central de Incendio en la oficina 217 del 2do piso de Paseo Colon Nº 982.
- Identificación, revisión y comprobación de las acciones realizadas en el Comité de Seguridad de la Información.
- Observación del acceso físico al área.
- Verificación de las actas efectuadas en el marco del citado Comité. Grado de cumplimiento alcanzado a las acciones planteadas con respecto a las metas planteadas originalmente.
- Elaboración del Informe de Auditoria correspondiente.

V. MARCO DE REFERENCIA

- **Ley N° 22.520,** Ley de Ministerios.
- **Ley Nº 24.156,** Ley de Administración Financiera y de los Sistemas de Control del Sector Público Nacional
- **Ley Nº 27.275,** Ley que tiene por objetivo garantizar el efectivo ejercicio del derecho a la información pública.

- **Decreto Nº 13/15**, en donde se atribuyen las competencias al Ministerio de Agroindustria.
- **Decreto Nº 117/16,** por el cual se instruye a todos los organismos dependientes del poder Ejecutivo Nacional a elaborar y presentar un "Plan de apertura de datos".
- **Resolución SGN Nº 107/98,** por la que se aprueban las "Normas Generales de Control Interno" **Resolución SIGN Nº 152/02,** por la que se aprueban las Normas de Auditoría Interna Gubernamental".
- **Resolución SGN Nº 48/05**, por la que se dictan normas de control interno de Tecnología de la Información.
- **Resolución SGN Nº 172/14**, por la que se modifican las "Normas Generales de Control Interno".
- **Disposición ONTI Nº 1/15**, por la cual se aprueba la Política de Seguridad de la Información Modelo**.**
- **Resolución MAGYP N° 302/10**, por la que se crea en el ámbito del MAGyP el Comité de Seguridad de la Información.
- **Resolución MAGYP Nº 1066/13**, por la que se sustituye el artículo 2do. de la Resolución MAGYP Nº 302/10.
- **Resolución MAGYP Nº 867/15:** por la que se dicta la Política de Seguridad del MA
- **Decisión Administrativa de la Jefatura de Gabinete de Ministros N° 669/04**, por la cual se establece que las máximas autoridades del Sector Público Nacional comprendidos en el Artículo 7° de esa medida deberán conformar en sus ámbitos un Comité de Seguridad de la Información integrado por las Direcciones Nacionales o Generales o equivalentes de la institución; en el ámbito del MA compuesto por dos (2) Directores Nacionales y/o Generales por cada Secretaría, por la Subsecretaría de Coordinación Técnica y Administrativa a propuesta de sus titulares y por el correspondiente señor Subsecretario , quien adicionalmente lo coordinará.
- **Disposición ONTI Nº 1/15**, por la cual se aprueba la Política de Seguridad de la Información Modelo**.**

- **Lineamientos SIGEN 2018,** por los cuales se aprueban los lineamientos estratégicos a utilizar en la Planificación Anual 2018.

VI. ACLARACIONES PREVIAS

La Disposición de la Oficina Nacional de Tecnologías de la Información (ONTI) Nº 1/15 expresa que la Seguridad de la información es un activo esencial y en consecuencia necesita ser protegido adecuadamente.

La política de seguridad de la información es el marco general establecido por las autoridades y define las pautas para preservar la seguridad de la información de una organización y de la cual que se derivan las normas y procedimientos operativos para implementar esas disposiciones. Se establecen y construyen en ella medidas de control y seguridad con el fin de proteger a la información de posibles riesgos o amenazas y además a contribuir al eficaz cumplimiento de los objetivos del organismo a la cual están dirigidas, determinando qué conductas en relación con los sistemas de información son permitidas y cuáles no.

En toda organización la información debe protegerse de cualquier divulgación o alteración no autorizada o pérdida, sea cual fuese el medio en el cual se encuentre. Una organización sin información no puede cumplir con las funciones para las cuales existe.

La información con la que cuenta el entonces Ministerio es de diferentes tipos, y una de las tareas fundamentales de toda organización es conocer la información que maneja, por lo cual debe tipificarla. Se considera a la información un activo más del mismo, siendo uno de los de mayor valor.

Si la información de una organización es conocida por terceros no autorizados, esto podría ocasionar daños considerables a la organización, como ser: pérdida de confiabilidad, de imagen, incumplimiento legal, etc.

El diseño de la política contendrá los lineamientos generales y debe ser seguida de una serie de normas y procedimientos detallados que se derivan de ella. Es decir, deberán existir procedimientos y normas, aceptadas, escritas, difundidas y controladas que materialicen la política para que no quede en una expresión de buenas intenciones.

Mediante, la DA N° 996/04 de la Jefatura de Gabinete de Ministros se requiere que los organismos desarrollen sus Políticas de Seguridad de la Información (PSI) en función a un Modelo que fuera aprobado por la Oficina Nacional de Tecnologías Informáticas

(ONTI) hasta el año 2015 y posteriormente, por una modificación de la estructuras del Estado Nacional, por la Dirección Nacional de Infraestructuras Criticas y Ciberseguridad, ambas dependientes de la Subsecretaria de Tecnologías y Ciberseguridad del Ministerio de Modernización (MM).

Esto refleja la importancia que ya hace años reviste la seguridad de la información en la administración pública, y la importancia de que cada organismo defina las pautas de seguridad con las cuales va a tratar su información.

El Comité de Seguridad de la Información es un cuerpo integrado por representantes de todas las áreas sustantivas del organismo, destinado a implementar la PSI y garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

En el ámbito del entonces MA dicho comité fue constituido el 26 de agosto de 2010 mediante la Resolución MAGYP N° 302/10, efectuándose la primera reunión el día 15 de octubre de 2010. Su conformación se detalla a continuación:

- Dos (2) Directores Generales o Nacionales por cada Secretaría.
- Dos (2) Directores de la ex Subsecretaría de Coordinación Técnica y Administrativa.
- El Subsecretario de la ex Coordinación Técnica y Administrativa
- El titular de la Unidad de Auditoría Interna (con voz, sin voto)

Su reglamento, aprobado en la segunda reunión el día 08 de marzo de 2011, establece la organización y funcionamiento de dicho comité y estipula reuniones ordinarias cada seis (6) meses. Desde entonces se ha reunido nueve (9) veces, siendo la última reunión llevada a cabo el día 27 de octubre de 2015. La conformación de dicho comité no ha sido revisada desde entonces.

FECHA	RESUMEN ACTAS
15/10/2010	• Designación de dos (2) firmantes del acta de la segunda reunión • Se entrega un Reglamento Interno de funcionamiento del Comité de Seguridad de la Información (CSI) del MA

FECHA	RESUMEN ACTAS
08/03/2011	• Se presentan sugerencias al Reglamento interno entregado en la primera reunión a fin de mejorar la redacción del mismo. Se debe adecuar a la Resolución N° 302/10. • Ampliación de diversos incisos del Artículo 3° del reglamento. • Se aprueba la versión definitiva del reglamento para trabajar.
09/09/2011	• Tratamiento preliminar para definir criterios para la política de acceso a Data Centers y Cuadros Técnicos del Ministerio
31/01/2014	• Análisis del Reglamento Interno del Comité y sus posibles modificaciones. Proyecto de Resolución tendiente a aprobar el documento "Uso de Recurso Informáticos y Compromiso de Confidencialidad". Se aprueba el documento de política de acceso planteado en reunión anterior. Se comparte la Disposición ONTI Nº 3/13, "Política de Seguridad de la Información Modelo".
11/03/2014	• Se aprueba el Reglamento Interno de Funcionamiento. Se trata la Disposición ONTI Nº 3/13, en relación a los tópicos y división del trabajo, definiéndose el armado de grupos.
23/05/2014	• Con la participación de representantes de la ONTI, quienes resaltan la importancia que la jurisdicción tenga una política de seguridad modelo. Se trata la temática en general para trabajar en la Política del Ministerio.
23/04/2015	• Se presenta una planilla modelo para empezar a relevar activos del Ministerio, de acuerdo a las prioridades Riesgo/Amenaza del mismo. Se remitirá un papel de trabajo de política de seguridad de la información a fin de evaluarla.
18/08/2015	• Se trata sobre el resultado del relevamiento de activos efectuado y además sobre el rol de cada área dentro de la Política de Seguridad de la Información; los Contratos de confidencialidad y su necesidad y la seguridad del sitio web institucional. Se señala que se está trabajando en una Resolución que contendrá la Política de Seguridad del Ministerio.

FECHA	RESUMEN ACTAS
27/10/2015	• Presentación y posterior aprobación del instructivo "Condiciones necesarias para el desarrollo y puesta en marcha de aplicaciones y servicios informáticos en MAGYP", a los fines de ser sometido a análisis y consideración del Comité. Su finalidad fue garantizar que se cumpla la integridad, disponibilidad y confidencialidad para el desarrollo de software y operaciones informáticas en el ex MAGYP, y comprendía las condiciones necesarias para desarrollar e implementar un software informático o servicio en la Dirección de Informática del Ministerio.

Fuente: Elaboración propia en base a las Actas emitidas.

El Comité es el único canal para realizar recomendaciones normativas a fin de asegurar la homogeneidad y unicidad de criterios y objetivos en la materia.

La Dirección de Informática del Ministerio de Agroindustria (DI) dependiente de la Subsecretaría de Control Administrativo (SCA), tiene como función primaria dirigir, optimizar y entender en todos los aspectos relativos a la seguridad de las Tecnologías de la Información y las Comunicaciones, asegurando la eficiente utilización de los sistemas y herramientas informáticas, incluyendo el establecimiento de planes de contingencia para los sistemas críticos, controlando periódicamente su funcionamiento.

En su respuesta por NO-2018-32702521-APN-DI-MA, la DI informa que el área de Seguridad Informática se encuentra actualmente en proceso de conformación y aprobación por parte de la SCA. Su responsable y los analistas que la integran tienen roles y aptitudes definidos, y deben contar con experiencia en:

- Auditorías/revisiones de sistemas
- Tareas de Seguridad
- Conocimiento sobre Políticas de Seguridad
- Conocimiento sobre Redes
- Conocimiento de la Infraestructura del Ministerio.
- Conocimiento sobre Herramientas de Monitoreo, control de alertas, etc.
- Conocimiento sobre Estándares de Seguridad.
- Conocimiento de la organización del MA y de la DI.

- Conocimientos generales de sistemas y afines.

Procedimientos existentes

Existen diferentes procedimientos que la DI posee en el marco de la PSI, objeto de esta auditoría, los que se detallan a continuación:

- Baja de usuarios MAGYP

Los derechos de acceso de un individuo a los sistemas y servicios de información deben revisarse tras la desvinculación o cambio de puesto. La baja de usuarios MAGyP ante desvinculaciones del personal, se solicitan de tres formas.

Si el modo de contratación del agente en cuestión es Ley Marco o Planta Permanente, se genera mediante una Comunicación Oficial (CCOO) del sistema de Gestión Documental Electrónica (GDE) desde la Dirección General de Recursos Humanos hacia la Dirección de Informática, solicitando la baja del usuario con nombre y apellido con el motivo de renuncia o rescisión a partir de una fecha determinada.

Si posee algún otro modo de contratación, el funcionario a cargo del área envía un mail a soporte@magyp.gob.ar informando la desvinculación de la persona en cuestión. El aviso de desvinculación además puede ser remitido por las autoridades de RRHH vía email al Director de Informática para dar curso a la baja de permisos.

- Cambio de área o pase interno

Por otro lado, se debe asegurar que los agentes realicen un cambio de área o pase interno de una manera ordenada. Para los usuarios MAGyP, el pedido de pase interno se genera mediante una Comunicación Oficial (CCOO) del sistema de Gestión Documental Electrónica (GDE), desde la Dirección General de Recursos Humanos hacia el responsable del área a la cual se realiza el pase interno del personal, con copia a la Dirección de Informática para que tome conocimiento y así poder proceder a la depuración de los permisos del usuario. Es preciso señalar que es condición necesaria informar tanto al área de RRHH y con copia a la Dirección de Informática para que esta intervenga en la depuración de permisos. En consecuencia, es posible que no todos los cambios de área sean acompañados de su correspondiente depuración de permisos.

- Depuración de cuentas inactivas

Además, se deben efectuar revisiones periódicas con el objeto de identificar y depurar cuentas inactivas. Dicho procedimiento se realiza a partir de la ejecución de una tarea diaria programada, la cual se ejecuta mediante un script (archivo de procesamiento por lotes) que realiza una consulta para comprobar todos los usuarios que no ingresaron al sistema en un período de 60 días.

- Gestión de contraseñas

La gestión de contraseñas de los sistemas informáticos del entonces Ministerio de Agroindustria se encuentra enmarcada dentro de los lineamientos de la Política de Seguridad de la Información establecida. Se establece un historial de las ultimas 24 contraseñas, para mejorar la seguridad y determinar un número de nuevas contraseñas únicas asociadas a una cuenta de usuario. **(Ver Anexo I).**

Riesgo, amenaza y control

El riesgo es una combinación de la probabilidad de ocurrencia de un evento y sus consecuencias o impacto, mientras que una amenaza es una causa potencial de un incidente no deseado, el cual puede ocasionar daños a un sistema u organización.

AMENAZAS	RIESGOS
Correos electrónicos del tipo phishing donde se intenta suplantar la identidad de una empresa u organismo legítimo, incluyendo URLs maliciosas, generalmente apuntando a solicitar información sensible del usuario, y adjuntos con malware.	Posibles incendios: La sala de equipos está ubicada en un ambiente resistente al fuego, con una salida de emergencia distinta a la principal, con un plan de evacuación formalizado y un sistema de extinción automático diseñado para prevenir el daño de la infraestructura.
Ataques a servicios publicados hacia internet, donde se intenta explotar alguna vulnerabilidad para poder realizar acciones no autorizadas sobre dichos sistemas	Posibles Inundaciones: La infraestructura crítica se encuentra elevada del suelo por un piso técnico protegiendo de esta forma al equipamiento en cuanto a inundaciones y goteras.

AMENAZAS	RIESGOS
Ataques de denegación de servicio (DDoS) que tienen como finalidad saturar un servicio hasta el punto de dejarlo fuera de funcionamiento.	Posibles cortes de suministro eléctrico: Los equipos están protegidos por sistemas de UPS que son mantenidos y probados de manera regular. Por otro lado además se cuenta con líneas diferenciadas eléctricas del generador principal del Ministerio en caso de corte de luz.
Equipos endpoint que de alguna forma terminan siendo infectados por malware en donde a veces pueden llegar a afectar a otros equipos de la red.	Posibles accesos indebidos a las salas de equipos: Todos los cuartos técnicos y Datacenters cuentan con sistemas de vigilancia que se encuentran monitoreando las 24hs alertando en caso de movimiento, y con control de accesos biométricos en todos sus accesos.
	Posibles cortes en la red de telecomunicaciones: Toda la red del ministerio posee un esquema redundante. Tanto en equipamiento de piso, como en los servicios de internet (Fibra Optica (FO) automática). De esta forma se evitan cortes en caso de que se dañe algún enlace entre equipos.

AMENAZAS	RIESGOS
	Posibles perdida de datos almacenados: Se realizan respaldos de manear regular en aplicaciones y servidores. Los mismos además se almacenan en otra ubicación física y protegida para favorecer el resguardo de la información en caso de desastre.

La DI tiene dentro de sus procesos desarrollados el manual de procedimiento "*PRC-CSSC-GSEG- Identificación Gestión y registro de riesgos informáticos*.

Procedimientos asociados a controles preventivos

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. La Dirección posee el documento "*Condiciones necesarias para el desarrollo y puesta en marcha de aplicaciones y servicios informáticos en MAGYP*", donde se establecen las pautas necesarias para disminuir los riesgos y garantizar que se cumplan los aspectos mínimos para el desarrollo de software, de acuerdo a la Política de la Seguridad de la Información.

El área de Seguridad Informática realiza diariamente un análisis en el tráfico de red para detectar anomalías en la misma. A fin de identificar desarrollos de software que no han sido llevados a cabo bajo proyectos propios, mediante dicho análisis es posible identificar servicios o dispositivos compatibles con el funcionamiento de sistemas informáticos. En el caso de detectarse uno, se procede a rastrear al usuario/área para que comuniquen su uso. Se debe señalar que en todos los casos u ocasiones se ofrece al usuario/área el alojamiento de esos servidores, servicios y/o aplicaciones en sitios destinados y acondicionados para tal fin, donde se brinda seguridad, integridad y disponibilidad de lo allí alojado.

Con la finalidad de mantener la continuidad de las actividades del organismo, la DI efectuó el procedimiento "*PRO.CA.SEG.01_ACCIÓN DE ALARMA DE INCENDIO".* En el mismo se designa a los responsables de su ejecución y se establece el curso de acción a tomar ante una alerta o alarma en la central de incendio de la sala de cómputos del entonces Ministerio.

Con el propósito de verificar este proceso, se efectuó una inspección ocular el pasado día 3 de agosto de 2018 junto con personal de la DI, visitándose dicha sala y constatándose que el control de acceso a la misma se realiza mediante un panel biométrico, y el acceso se encuentra restringido exclusivamente a personal de la DI.

El interior de la sala se encuentra monitoreado con cámaras de seguridad, la temperatura es regulada con aire acondicionado e incluye un sistema de supresión de fuego y detectores de humo. Esta es una condición necesaria que ambos detectores detecten humo para que se dispare la alerta. En caso de existir fuego, se corta la electricidad de la sala y se dispara el sistema de supresión de fuego.

En el marco de la misma inspección ocular se visualizó además el almacén de cintas de resguardo, que comprende el procedimiento "*PRO.INF.01-Generación y resguardo de backups"*. En dicho proceso se encuentran establecidas pautas necesarias para la correcta generación y respaldo de la información trascendente del organismo.

Del examen realizado se verificó que las cintas se encuentran en repisas, con su identificación visible de acuerdo a la nomenclatura definida en el procedimiento. El cuarto se encuentra monitoreado por cámaras de seguridad, con detector de agua y un equipo des-humificador. Para resguardar las cintas de carácter crítico se emplea una caja de seguridad ignífuga, protegida con una combinación conocida únicamente por los responsables del procedimiento para su efectivo resguardo.

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. El documento "*Condiciones necesarias para el desarrollo y puesta en marcha de aplicaciones y servicios informáticos en MAGYP*" establece las pautas necesarias para minimizar los riesgos y garantizar que se cumplan los aspectos mínimos para el desarrollo de software, de acuerdo a la Política de la Seguridad de la Información. El área de Seguridad Informática realiza diariamente un análisis en el tráfico de red para detectar anomalías en la misma. A fin de identificar desarrollos de software que no han sido llevados a cabo bajo proyectos propios, mediante dicho análisis es posible identificar servicios o dispositivos compatibles con el funcionamiento de sistemas informáticos. Una vez detectados, se rastrea a los usuarios responsables para que informen su uso. En todas las ocasiones se ofrece al área el alojamiento de esos servidores, servicios y/o aplicaciones en sitios destinados y acondicionados para tal fin, donde se brinda seguridad, integridad y disponibilidad de lo allí alojado.

Finalmente, a fin de lograr conciencia sobre la temática y como parte de una exitosa implementación de la PSI, es necesaria la difusión efectiva de la misma a todos los agentes que forman parte del organismo.

De la información remitida por la DI, desde tal fecha se efectuaron cinco (5) comunicaciones masivas a los agentes del organismo en relación a lo anteriormente expresado.

Actualmente se encuentran en proceso de diagramación nuevas capacitaciones, haciendo hincapié en temas como phishing (suplantación de identidad), scam (estafas), claves seguras y navegación en general.

ANALISIS F.O.D.A

FORTALEZAS

- El Organismo cuenta con un Comité de seguridad de la información.
- Existencia de una Política de Seguridad de la Información.
- Compromiso de funcionarios públicos con las Políticas citadas.

OPORTUNIDADES

- Convocar a reuniones del Comité de seguridad de la información
- Generación de un mecanismo institucional de transmisión de información cotidiano o amigable hacia los agentes del organismo.

DEBILIDADES

- Baja difusión de las Políticas de Seguridad de la Información entre los agentes del organismo.
- Implementación de las prácticas sin planificación debidamente aprobada.

AMENAZAS

- Posibilidad de acceso no autorizado a una red o equipos informáticos de terceros ajenos al organismo.
- Robo de información sensible o confidencial.
- Pérdida o mal uso de la información por parte de agentes del organismo.

VII. HALLAZGOS, IMPACTO Y RECOMENDACIONES

1. Inactividad del Comité de Seguridad de la Información.

De la respuesta dada por el auditado se observó que la última reunión del Comité fue efectuada el día 27 de octubre de 2015, transcurridos casi treinta y cuatro (34) meses a la fecha del presente sin que se impulse la prosecución del mismo.

Se resalta que la trascendencia y criticidad de la información del entonces MA determinaron oportunamente la creación del mentado Comité a fin que participe en toda cuestión relacionada directamente con la Seguridad de la Información. Siendo éste, el único ámbito mediante el cual se debe plasmar modificaciones normativas de acuerdo a lo establecido en su formulación.

Impacto: Alto

Recomendación: Se deben realizar las acciones necesarias tendientes a impulsar las reuniones del Comité de Seguridad de la Información con el objeto de continuar la implementación de la Política de Seguridad de la Información en el organismo, en cumplimiento de la normativa vigente y específica en la materia.

Opinión del Sector auditado: Sin respuesta del sector auditado.

2. Falta de actualización de la lista de sistemas informáticos desarrollados que se encuentran fuera del ámbito y control de la DI.

Se constató mediante el cruce de información con auditorías ya efectuadas en planificaciones correspondientes al año en curso, año 2017 y otros, que el entonces MA tiene sistemas desarrollados por varias áreas que no cuentan con el apoyo de la DI y que no se encuentran contemplados en el informe “Servicios fuera del control de la DI” provisto durante la presente auditoría. (Ver anexo II punto a).

Impacto: Alto

Recomendación: Se sugiere realizar un relevamiento exhaustivo a fin de identificar aquellos desarrollos de software realizados sin la participación o supervisión de la DI. Procediendo a realizar un análisis de vulnerabilidad en los mismos.

En otro orden de ideas, esta UAI considera trascendental que ante situaciones en las que la DI se vea imposibilitada de satisfacer las solicitudes de desarrollo de software, comunique al área requirente mediante nota formal las condiciones mínimas necesarias para el desarrollo y que efectúe tareas de supervisión de la puesta en producción.

Opinión del Sector auditado: Sin respuesta del sector auditado.

3. **Falta de adecuación del Comité de Seguridad de la Información a la estructura vigente del MA.**

Al encontrarse sin actividad el Comité desde el mes de octubre de 2017, se encuentra desactualizada la estructura que se da cuenta en él. Debe reiterarse que el citado Comité es el único canal para realizar recomendaciones normativas.

Impacto: Medio

Recomendación: Se sugiere proceder a adecuar y modificar el mismo de acuerdo al Decreto Nº 174/18 y la Decisión Administrativa de la Jefatura de Ministros Nº 324/18.

Opinión del Sector auditado: Sin respuesta del sector auditado.

4. **Falla en la depuración de permisos por cambio de área.**

Del examen realizado, se observó la posibilidad que no todos los cambios de área sean acompañados de su correspondiente depuración de todos los permisos, entre los que se incluye la baja de discos de grupo pertenecientes al área abandonada.

Impacto: Medio

Recomendación: Se debe capacitar y profundizar en las acciones que el área de RRHH es responsable a fin de realizar en tiempo y forma la actividad observada.

Opinión del Sector auditado: Sin respuesta del sector auditado.

5. **Debilidad en la difusión de las políticas de seguridad de la información del organismo.**

La Disposición ONTI Nº 1/15 base normativa de la Resolución MAGyP Nº 867/15 establece que las políticas de seguridad de la información deben ser conocidas y cumplidas por toda la planta de personal del Organismo, tanto se trate de funcionarios políticos como técnicos, y sea cual fuere su nivel jerárquico y su situación de revista. (Ver anexo II punto c)

Impacto: Bajo

Recomendación: Se sugiere realizar comunicaciones masivas a fin de lograr transmitir la importancia sobre la seguridad de la información.

Opinión del Sector auditado: Sin respuesta del sector auditado.

6. **Falta de revisión, aprobación formal y actualización de la normativa vigente de los procesos de la Dirección de Informática.**

Hay procesos de la DI que no cumplió el régimen de revisión, no se encuentran aprobados formalmente, además de encontrarse desactualizados de la normativa vigente (ver anexo II – Evidencia).

Impacto: Bajo

Recomendación: Se sugiere proceder a la aprobación formal de los procesos actualizándolos previamente a la actual estructura del Ministerio (Ejemplo: "Proceso de Generación y Resguardo de Backups"- "El propietario del presente proceso es la Dirección de Informática del Ministerio de Agricultura, Ganadería y Pesca –MAGyP").

Opinión del Sector auditado: Sin respuesta del sector auditado.

VIII. RESULTADOS OBTENIDOS DEL CUMPLIMIENTO DE OBJETIVOS ESTRATEGICOS SGN

En el marco de los Lineamientos de Auditoría 2018 para la elaboración del Plan Anual de Auditoría, la Sindicatura General de la Nación definió objetivos estratégicos que abordan diferentes temáticas, debiendo las Unidades de Auditoría Interna realizar el relevamiento correspondiente.

Esta Unidad de Auditoria Interna relevó los siguientes objetivos:

- Relevamiento del Estado de Aplicación de Sistemas Normalizados de Aplicación.
- Responsabilidad Social.
- Responsabilidad Ambiental.
- Costos de la No Calidad.
- Corrupción Cero.
- Identificación de Centros de Responsabilidad de Procesos.
- Construcción de Programas de Incentivos a la Productividad.

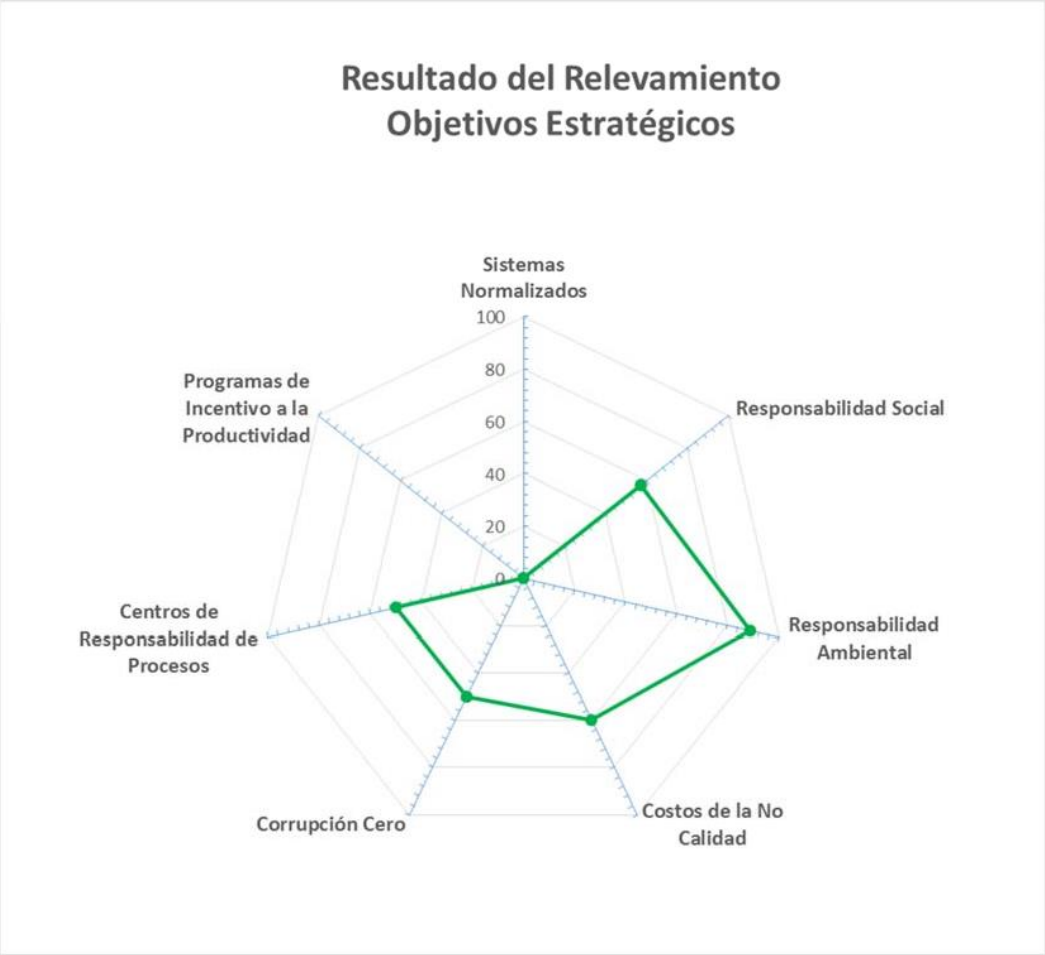
A tal efecto se exponen a continuación los resultados del análisis efectuado en función de la información suministrada por el área auditada referida a los objetivos mencionados.

Políticas de Seguridad de la Información

Número	Objetivo	Grado de Implementación (%)
1	Sistemas Normalizados	0,00
2	Responsabilidad Social	57,14
3	Responsabilidad Ambiental	88,89
4	Costos de la No Calidad	60,00
5	Corrupción Cero	50,00
6	Centros de Responsabilidad de Procesos	50,00
7	Programas de Incentivo a la Productividad	0,00
Porcentaje del grado de implementación global de los Objetivos		**43,72**

Fuente: Elaboración propia en base a la información enviada por el área auditada.

✔ : valores mayores o iguales a 75%
! : valores mayores o iguales a 40% y menores que 75%
✘ : valores menores a 40%



Atento a lo expuesto, se observa que el área auditada no cuenta con Sistemas Normalizados y con Programas de Incentivo a la Productividad.

En cuanto a los objetivos de Responsabilidad Ambiental, Social y Costo de la No Calidad se verifica un grado de implementación aceptable.

En virtud de lo observado, se considera adecuado establecer mecanismos con el objeto de mejorar la implementación global de los objetivos. (Ver Anexo II)

IX. CONCLUSIÓN

Las tareas se realizaron en un adecuado ambiente de control interno de acuerdo a los lineamientos impartidos por la Sindicatura General de la Nación mediante Resolución SGN Nº 152/02.

Mediante la nota NO-2018-41218154-APN-UAI#MA se remitió el presente informe para que el área auditada exponga su opinion respecto de las observaciones detalladas por esta UAI, en la cual textualmente se expresaba: "(*…) Vencido dicho plazo, y no habiéndose otorgado formalmente una prórroga al mismo, el informe se emitirá destacando la ausencia de respuesta de dicha opinión a cada observación formulada. Se adjunta el correspondiente informe para su descargo (…)".*

Si bien a la fecha de la emision del presente informe de auditoría, no se recepciono respuesta alguna por parte del auditado, las observaciones expuestas seran objeto de revision al efectuarse las tareas de seguimiento de observaciones pendientes.

Es importante mencionar que la información es un recurso, un activo de la organización que posee valor para el Organismo, por lo que su protección a través de una adecuada Política de Seguridad Informática es necesaria a fin de mantener y preservar la seguridad del mismo.

Atento a lo expuesto y en relación a los desvíos observados, se considera necesario y de gran utilidad impulsar el Comité de Seguridad de la Información en el ámbito de la jurisdicción a fin de cumplir con los objetivos de la ONTI y la normativa vigente, Ello minimizará los riesgos y contribuirá al cumplimiento eficiente de los objetivos.

Corresponde por último señalar que las tareas de auditoría y la redacción del presente informe definitivo tuvieron lugar con anterioridad a la asunción, el día 3 de septiembre del 2018, a mí actual cargo de Auditora Interna Titular, conforme lo dispuesto por Resolución SIGEN Nº 143 de fecha 24 de agosto del corriente.

En este sentido, se hace constar que, con la limitación de responsabilidad que la situación descripta conlleva, se suscribe el presente a los fines de posibilitar la correcta ejecución de la Planificación Anual de esta Unidad de Auditoría Interna aprobada para el ejercicio 2018.

Buenos Aires, 07 de noviembre de 2018

SANTARELLI Giselle Eliana

Firmado digitalmente por SANTARELLI Giselle Eliana
Nombre de reconocimiento (DN): serialNumber=CUIL 27266203700, c=AR, cn=SANTARELLI Giselle Eliana
Fecha: 2018.11.07 16:59:27 -03'00'

ANEXO I – EVIDENCIA

a.-

"2015 - AÑO DEL BICENTENARIO DEL CONGRESO DE LOS PUEBLOS LIBRES"

Ministerio de Agricultura, Ganadería y Pesca

Acta N° 9
27 OCT 2015

ACTA DE LA NOVENA REUNIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DEL MAGYP

En la Ciudad Autónoma de Buenos Aires, a los 27 días de octubre de 2015, se reúnen los integrantes del Comité de Seguridad de la Información del Ministerio de Agricultura, Ganadería y Pesca, conforme la convocatoria dispuesta por el señor Subsecretario de Coordinación Técnica y Administrativa.
Siendo las 11.15 hs., se declara iniciada la presente reunión con la presencia de los siguientes miembros del Comité, a saber: Arquitecto Gustavo FERNÁNDEZ, Ingeniero Alejandro CRISAFULLI, Señor Martín SARRIES, Doctora Raquel SANTOS LAGUARDIA, Marina ROCHETEAU, Carla Estefanía SEAIN; Licenciado Luciano ZARICH, Ingeniero José María MONES CAZÓN, Manuel Enrique PEDREIRA, de acuerdo a lo establecido por la Resolución MAGYP N° 302/10 y sus modificatorias, y se procede a dar apertura a la reunión:

1.- Designación de DOS (2) representantes que firmarán el acta.
Se designan al Ingeniero Alejandro CRISAFULLI y a la Doctora Raquel SANTOS LAGUARDIA para firmar en representación de los miembros asistentes.

2.- Presentación y posterior aprobación del instructivo "CONDICIONES NECESARIAS PARA EL DESARROLLO Y PUESTA EN MARCHA DE APLICACIONES Y SERVICIOS INFORMÁTICOS EN MAGYP" presentado por la Dirección de Informática, que forma parte integrante de la presente acta.
Las autoridades de la DI presentan el documento referido a los fines de ser sometido a análisis y consideración del Comité. El mismo tiene como finalidad garantizar que se cumpla la integridad, disponibilidad y confidencialidad para el desarrollo de software y operaciones informáticas en el MAGYP, y comprende las condiciones necesarias para desarrollar e implementar un software informático o servicio en la Dirección de Informática del Ministerio de Agricultura, Ganadería y Pesca.
Se distribuye entre los miembros presentes y se acuerda:

a) La difusión del documento vía mail a todos los miembros.

b) La revisión x parte de los miembros antes del viernes 30 de octubre de 2015, fecha en la cual, dicho documento será aprobado de forma automática, de no mediar objeciones por parte de los miembros.
c) Asimismo, si mediaran las mismas, será aprobado el documento en aquellas cuestiones que no fuera menester modificar o consensuar.
d) La aprobación posterior mediante el procedimiento normativo vigente y en el marco de la Política de Seguridad del MAGYP.

3.- E – COMDOC (Comdoc IV)

Asistieron José LEZAMA y Guillermo MALDONADO de la ONTI de la JGM para presentar las funcionalidades del Sistema E-COMDOC.

Luego de dicha presentación y de evacuadas las dudas se conviene la necesidad de implementar el E-COMDOC en el MAGYP con todas sus prestaciones.

Asimismo, se acuerdan las siguientes responsabilidades, dentro de las competencias de las respectivas áreas:

- Responsable funcional de la implementación: DDYME
- Soporte normativo de la implementación: DDYME en colaboración con la DGAJ
- Responsable técnico de la implementación y soporte: DI
- Responsable de capacitación y procesos: DGRRHH

4. – OTROS TEMAS

Se pide la difusión vía mail del resultado del relevamiento de activos.

Dicha tarea será llevada a cabo mediante el Responsable de Seguridad.

Los miembros convienen que de ahora en adelante, los documentos que se sometan a aprobación vía mail serán aprobados, excepto oposición en concreto, en el plazo de 30 días corridos a contar de su envío.

Asisten en representación:

Oscar GONZALEZ en representación de la SECRETARÍA DE AGRICULTURA,

"2015 - AÑO DEL BICENTENARIO DEL CONGRESO DE LOS PUEBLOS LIBRES"

Ministerio de Agricultura, Ganadería y Pesca

GANADERÍA Y PESCA.
Martín LIGUORI en representación de la Dirección General de Asuntos Jurídicos.
Erica ANDERSON atento a la temática vinculada a los procesos en el E-COMDOC.

Siendo las 13.00, se da por finalizada la novena reunión del Comité de Seguridad de la Información del Ministerio de Agricultura, Ganadería y Pesca.

Dra. RAQUEL SANTOS LAGUARDIA
DIRECTORA
DE DESPACHO Y MESA DE ENTRADAS
MINISTERIO DE AGRICULTURA GANADERIA Y PESCA

Ing. ALEJANDRO CRISAFULLI
DIRECTOR DE INFORMATICA
MINISTERIO DE AGRICULTURA, GANADERIA Y PESCA

b.- Servicios fuera de control de la Dirección de Informática.

El área de Seguridad Informática diariamente realiza análisis en el tráfico de red para detectar anomalías en la misma. De estos análisis surgen a veces algunos dispositivos con servicios de sharing, http, o bases de datos habilitados en donde se rastreó a los usuarios responsables para que informen su uso.

En todas las ocasiones se ofrece al área el alojamiento de esos servidores, servicios y/o aplicaciones en sitios destinados y acondicionados para tal fin, donde se brinda seguridad, integridad y disponibilidad de lo allí alojado.

Actualmente se identificaron dos (2) dispositivos con servicios, aplicaciones y características propias de un servidor:

1. El área Dirección Nacional de Control Comercial Agropecuario sito en el edificio de Azopardo 1025. Los mismos poseen un equipo con varios servicios. Los mismos fueron contactados a fines de regularizar la situación sin respuesta al momento de esta auditoría.
2. La Dirección Nacional de Producción de Alimentos y Bebidas, poseen un equipo donde ejecutan una máquina virtual con una base de datos donde guardan información relacionada al área y ejecutan reportes. (Actualmente se está migrando al Datacenter principal del Ministerio para alojar dicha base de datos)

Extraído del INFORME UAI-MA N° 024-001/2018 - PROGRAMA 46 - POLÍTICAS PARA PEQUEÑOS Y MEDIANOS PRODUCTORES Y DESARROLLO TERRITORIAL ACTIVIDAD 02 - FORMULACIÓN DE POLÍTICAS PARA EL DESARROLLO TERRITORIAL. PROGRAMA AGROEMPRENDE "INNOVANDO EN EL TERRITORIO".

c.-

Ministerio de Agroindustria
Presidencia de la Nación
Subsecretaría de Coordinación Administrativa
DIRECCIÓN INFORMÁTICA

COMUNICACIONES DE BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN

Se detallan los flyers y templates utilizados para las comunicaciones masivas.

Ministerio de Agroindustria
Presidencia de la Nación
Subsecretaría de Coordinación Administrativa
Dirección Informática

¿Qué es el Phishing?

Phishing es una forma de engaño mediante la cual se envía un mensaje ("anzuelo") a una o varias personas con el fin de convencerlas para que revelen datos personales. Luego, estos son utilizados para realizar acciones fraudulentas tales como transferencias de fondos de su cuenta bancaria, compras con tarjetas de crédito u otras acciones delictivas

Medidas de prevención

Si recibís algún mensaje o correo electrónico que te resulte sospechoso (que solicite información personal o financiera o te invite a acceder a un sitio web a través de un enlace, por ejemplo) no lo abras, borralo

No accedas a tu correo electrónico desde lugares públicos (cibercafés, locutorios etc.). Las PCs instaladas podrían contener software o hardware malicioso destinado a capturar tus datos personales

No descargues ni abras archivos de fuentes que no conocés. Estos podrían contener virus o software malicioso que podrían permitir a un atacante acceder a tu computadora

Por último, recordá que la Dirección de Informática nunca te solicitará información sensible como contraseñas vía correo electrónico

Por cualquier consulta, envianos un correo a soporte@magyp.gob.ar o llamanos al 42600

Dirección de Informática
Subsecretaría de Coordinación Técnica y Administrativa
Ministerio de Agroindustria
Presidencia de la Nación

Ministerio de Agroindustria
Presidencia de la Nación

Subsecretaría de Coordinación Administrativa

Dirección de Informática

Buenos Aires, 15 de mayo de 2017

Estimados:

Como es de público conocimiento, están sucediendo una serie de ciberataques, que han afectado a distintas instituciones y empresas en más de ciento cincuenta países. Se espera que esto continúe en los próximos días.

Estos ciberataques son producidos por un software malicioso o virus llamado WCry, WannaCry, WanaCrypt0r, WannaCrypt o Wana Decrypt0r de muy alta peligrosidad, que ingresa en el sistema operativo inutilizando la información del equipo sin posibilidades de recuperarla.

En este marco, el equipo de la Dirección de Informática ha tomado las medidas necesarias para que el mismo no se filtre y a su vez solicita a todos los usuarios del Ministerio que tomen las precauciones necesarias que enumeramos a continuación para colaborar con este trabajo.

Recomendaciones

Guardá tus archivos más importantes en los discos compartidos

No abras correos de personas o instituciones desconocidas ni descargues adjuntos extraños

Si detectás algo sospechoso en tu PC no dudes en avisarnos

La Dirección de Informática nunca te solicitará información sensible como contraseñas vía correo electrónico, así como tampoco que actualices información por medio de un link

Por cualquier consulta, envíanos un correo a soporte@magyp.gob.ar o llamanos al 42600

Estamos a tu disposición

Dirección de Informática
Subsecretaría de Coordinación Técnica y Administrativa

Ministerio de Agroindustria
Presidencia de la Nación

Ministerio de Agroindustria
Presidencia de la Nación
Subsecretaría de Coordinación Administrativa

Seguridad Informática
Información para el usuario

¿Cómo armar una contraseña segura?

Una clave segura está compuesta por al menos 8 caracteres combinados entre mayúsculas, minúsculas, números y símbolos.

NO debe contener datos personales ni familiares. Ya sean fechas importantes, número de documento, nombres, direcciones, lugar de trabajo, etc.

Algunos ejemplos de contraseñas seguras son:
Calcular-dato253
2017.Ordenador$
B!cicl3tA.982

Recordá que la Dirección de Informática NUNCA te solicitará información sensible como contraseñas vía correo electrónico.

Por cualquier consulta, envíanos un correo a soporte@magyp.gob.ar o llamanos al 42600

Dirección de Informática
Subsecretaría de Coordinación Técnica y Administrativa

ANEXO II – CUMPLIMIENTO DE OBJETIVOS ESTRATÉGICOS SGN.

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
1	Relevamiento del estado de aplicación de Sistemas Normalizados de Gestión, acreditaciones, etc.	Por ejemplo: Calidad-Procesos ISO 9.001. Ambiental ISO 14.001. Anticorrupción ISO 37.001. Responsabilidad Social ISO 26.000 (no certificable).	a) ¿Posee sistemas / procesos certificados a nivel internacional?	X				
			b) ¿Se trata de un Proceso Principal (*)?				X	
			c) ¿Se trata de un Proceso Secundario (*)?				X	
			d) ¿En qué etapa se encuentra la certificación?: d.1) Iniciado				X	
			d.2) En Proceso				X	
			d.3) Finalizado				X	
			d.4) Certificado				X	
2	Responsabilidad Social	Relevamiento del ambiente laboral en cuanto a su crecimiento,	a) ¿El área realiza alguna actividad de Responsabilidad Social?		X			

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
		capacitación, pertenencia, equidad de género, cumplimiento de cupo de discapacitados, etc.	b) ¿Sabe si el MA cuenta con Código de conducta?				X	Se desconoce
			c) ¿Sabe si el MA cuenta con Lista de Valores?				x	Se desconoce
			d) ¿Conoce si el área cuenta con alguna certificación ya sea ISO 9001; ISO 14001; Otras?			x		
			e) ¿Sabe si el MA tiene algún documento que haga referencia a políticas de igualdad efectiva entre hombre y mujer, y conciliación de la vida familiar y laboral?				x	Se desconoce

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
			f) ¿Se identifica usted con la mayoría de los valores del área del MA a la cual pertenece?	x				
			g) Considera usted que la cultura del área del MA a la cual pertenece tiene en consideración los valores que se señalan: g.1) Tiempo familiar (empleado fuera de su horario laboral, o pactar reuniones que finalizan pasado el horario laboral) Indique además frecuencia de ello.	x				
			g.2) Formación igual para ambos sexos.	x				

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
			g.3) Acciones para evitar el acoso o situaciones de discriminación	x				
			g.4) Igualdad de oportunidades	x				
			h) El MA cuenta con guardería para los hijos de los agentes:					
			h.1) ¿Algún agente del área hace uso de este servicio?	x				
			h.2) ¿El valor es accesible?	x				
			h.3) ¿La posibilidad de ingreso es general?	x				
			i) Durante el tiempo que trabaja en el área tuvo algún inconveniente o situación asociada a:					

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
			i.1) Discriminación por edad, sexo, religión.				x	
			i.2) Discriminación en la posibilidad de acceder a algún curso de formación o tareas.				x	
			i.3) Acoso laboral.				x	
			i.4) Acoso sexual.				x	
			j) En relación a si es un Programa específico ¿Se buscó fortalecer el apoyo productivo y promoviendo el desarrollo regional? Indicar a quien:					
			j.1) Comunidades originarias				x	

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
			j.2) Familias en condiciones de vulnerabilidad social				**x**	
			j.3) Pequeño productor agrícola ganadero				**x**	
			k) Indique a que objetivo se dirigen esas acciones: k.1) Mejorar la calidad de vida.				x	
			k.2) Dar agua.				x	
			k.3) Mejorar el hábitat.				x	
			k.4) Otorgar mismas oportunidades				x	
			k.5) Empleo.				x	
			k.6) Capacitación.				x	

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
3	Responsabilidad ambiental	Relevamiento de Pasivos Ambientales e impacto ambiental (contaminación de aire, agua y tierra). Aplicación de la Guía de Auditorías Ambientales SIGEN- mayo 2014.	a) En relación al papel que utilizan en el área, indique: ¿La impresión es doble faz?	x				
			b) En caso que responda NO al punto anterior, puede decirnos si debe a: b.1) No hay impresora que imprima así.					
			b.2) No tiene configurada la impresión de ese tipo.					
			b.3) No se lo piden de esa forma.					
			c) El papel que no sirve se tira en: c.1) Contenedor especial para reciclado posterior.	x				

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
			c.2) En tacho común.					
			d) ¿Cuál es el medio de comunicación que utiliza habitualmente?: d.1) GDE	x				
			d.2) Correo electrónico.	x				
			d.3) Lync	x				
			d.4) Teléfono.	x				
			d.5) Memo impreso.			x		
			d) ¿Verifica que ha cerrado las canillas de agua correctamente	x				
			f) ¿En caso de detectar pérdidas y goteras de agua, avisa al servicio de mantenimiento?	x				
			g) Uso responsable de insumos y electricidad:					

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
			g.1) ¿Agita el tóner cuando la impresora avisa que el nivel está bajo?	x				
			h) ¿Apaga los dispositivos electrónicos al término de la jornada laboral?:	x				
			h.1) Computadoras	x				
			h.2) Impresoras	x				
			h.3) Fotocopiadoras	x				
			h.4) Aires acondicionados	x				
			h.5) ¿Utiliza el aire acondicionado en 24º?	x				
			h.6) ¿Se encienden y apagan las luces en intervalos de menos de treinta minutos?	x				

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
			h.7) ¿Conoce si las luces utilizadas son de bajo consumo?	x				
			i) Conoce la forma en que se almacenan los residuos tóxicos como:					
			i.1) Tubos fluorescentes agotados			x		
			i.2) Aerosoles				x	
			i.3) Pilas				x	
			i.4) Baterías				x	
4	Costos de la "NO CALIDAD"	Relevamiento de las 10 (diez) acciones u omisiones que generan los mayores costos. Ejemplo:	a) ¿El proceso administrativo del sector excede las exigencias de lo requerido de acuerdo a la normativa que lo regula?			x		

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
		procesos administrativos que exceden las exigencias de lo requerido en las leyes que regulan la materia.	b) ¿El sector cuenta con Manuales de procedimientos aprobados que permitan al personal trabajar en forma eficiente?	x				
			c) ¿Las adquisiciones se realizan en forma oportuna?	x				
			d) ¿Poseen tecnología obsoleta?	x				
			e) ¿Falta adquisiciones que sean imprescindibles en el sector y no obstante disponen de presupuesto?				x	
			f) ¿Poseen sistemas informáticos o equipos nuevos sin instalarlos?				x	

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
			g) ¿Poseen sistemas informáticos o equipos rotos o dañados que no hayan sido enviados a reparación en forma oportuna?	x				
			h) ¿Poseen exceso de personal, generando tiempos ociosos?				x	
			i) ¿El personal se encuentra debidamente capacitado a fin de que el trabajo diario se realice en tiempo oportuno?	x				
			j) ¿Posee el área personal profesional acorde a las tareas del sector?	x				

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
5	Corrupción Cero	* Corrupción cero	a) ¿Se le comunicó alguna información respecto al tema de corrupción?			x		
			b) En caso afirmativo responda, dicha información provino de: b.1) Publicidad en el edificio			x		
			b.2) Recursos Humanos				x	
			b.3) Superior Directo				x	
			b.4) Otros				x	
			c) ¿Realizó alguna capacitación anti fraude? ¿O relativa a corrupción cero?			x		

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
			d) ¿Ante un hecho o duda ética en este sentido, sabría a quién recurrir para comentarlo?	x				
			e) ¿Conoce que puede hacer denuncias en forma anónima y confidencial?	x				
			f) ¿Usted cree que puede hablar libremente con su superior, o compañeros de trabajo sobre este tema?	x				
			g) ¿Existe una correcta segregación de funciones en el área?	x				
			h) ¿Qué cree usted que podría ayudar disminuir la corrupción en la contratación pública?	x				

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
			a) El Área cuenta con un Código de Conducta?			x		
			b) En caso que responda SI a la pregunta anterior, El Código es de conocimiento de todo el personal del Área?				x	
		* Código de conducta.	c) El personal ha firmado, al momento de su incorporación, una Constancia de Conocimiento y Adhesión al cumplimiento?				x	
			d) Existe un programa de Difusión de las pautas del Código de Conducta?				x	

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
		* Mapa de riesgo.	a) ¿El Área posee una Mapa de Riesgos del sector?			x		
			b) En caso afirmativo responda: ¿Se actualiza periódicamente ?					
			b.1) ¿Es de conocimiento de todo el personal?				x	
			b.2) ¿Cómo se asegura que se cumpla?				x	

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
7	Identificación de Centros de Responsabilidad de Procesos	Coherencia organizacional en cuanto a vincular Responsables de Procesos con Responsables de Costos.	a) Posee indicadores de resultados a fin de verificar el impacto producido? Ya sean indicadores de gestión, informes de gestión, informes de cumplimiento de metas y cualquier otro documento que reflejen logros.				x	
			b) ¿Realizan una cuantificación de costos/ presupuesto?				x	

Políticas de Seguridad de la Información

Ítem	Objetivo Estratégico	Aspectos / Referencias	Cuestionario	Si	Detalle	No	N/A	Comentarios
8	Construcción de programas de incentivos a la productividad	Propuestas de "Prácticas Seguras" que concilian intereses de los actores. Encuestas de satisfacción de los productos/servicios.	a) En caso de poseen indicadores responda: ¿Se efectúa la medición de los mismos?				x	

ANEXO III – EQUIPO DE TRABAJO

Auditor Interno Titular

Cdra. Giselle Santarelli

Supervisora de Procesos y Sistemas

Dra. Lisa María Mac Donnell

Auditores:

Sr. Martin Castilla

Sr. Gianfranco Spagnuolo