Dirección Nacional de CORREOS del PARAGUAY

GOBIERNO NACIONAL

Paraguay de la gente

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Dirección Nacional de Correos del Paraguay

"DINACOPA"

mecip 2015

Norma de Requisitos Mínimos para Sistemas de Control Interno

Asunción - Paraguay 2023

Abg. Luis Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

Dirección Nacional de CORREOS del PARAGUAY

GOBIERNO NACIONAL

RESOLUCIÓN Nº 1137 /2023/DG/SG/MECIP

POR LA CUAL SE APRUEBA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÒN EN LA DIRECCIÒN NACIONAL DE CORREOS DEL PARAGUAY- DINACOPA.-

Asunción, 16 de Junio de 2023.-

VISTO: *Que en fecha 12 de febrero de 2021, se dictó el Decreto Nº 4845/2021, "POR LA CUAL SE REGLAMENTA LA LEY Nº 6562/2020 "DE LA REDUCCIÒN DE LA UTILIZACIÒN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL".-*

CONSIDERANDO*: Que, en fecha 27 de octubre de 2022, se dictó Resolución N°1478/2022/DG/SG/MECIP, "POR LA CUAL SE CONFORMA EL COMITÉ MULTIDISCIPLINARIO DE LA DIRECCIÓN NACIONAL DE CORREOS DEL PARAGUAY , EN EL MARCO DE LA IMPLEMENTACIÓN DE LA LEY N°6562/2020 "DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL" Y EL DECRETO N° 4845/2021 "POR EL CUAL SE REGLAMENTA LA LEY N° 6562/2020" "DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL".-*

Que, en fecha 27 de octubre de 2022, se dictó Resolución N° 1479/2022/DG/SG/MECIP, "POR LA CUAL SE ADOPTA, LO DISPUESTO EN LA LEY N° 6562/2020 "DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL" Y EL DECRETO N° 4845/2021 "POR EL CUAL SE REGLAMENTA LA LEY N° 6562/2020" "DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL".-

Que, la Seguridad de la Información consiste en la protección de los activos de información asegurando el acceso a los datos, garantizando la integridad, confiabilidad, disponibilidad y autenticidad de la información.-

Que, ante la existencia del Plan Nacional de Ciberseguridad configurándose como documento estratégico que sirve como fundamento para que Paraguay establezca una política pública de ciberseguridad, que integrando a todos los sectores involucrados en el desarrollo de las tecnologías de la información y comunicación (TIC), permita el crecimiento económico y la maximización de los beneficios de las mismas, logrando un ciberespacio más estable, seguro, confiable, y resiliente en base a políticas gubernamentales y nacionales que establece las líneas de acción a ser adoptadas por un país para fortalecer la seguridad de sus activos críticos y lograr un ciberespacio seguro, confiable y resiliente.-

Lic. Fernando Riveros

Que, resulta necesario la elaboración de la normativa aplicable a la realidad Institucional en la DINACOPA y tomando en cuenta los estándares, resoluciones y buenas prácticas emitidos por el Mitic.-

Abg. José Fernando Servín
Director General
DINACOPA

Dirección Nacional de CORREOS del PARAGUAY

GOBIERNO NACIONAL

RESOLUCIÓN Nº 1137/2023/DG/SG/MECIP

POR LA CUAL SE APRUEBA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÒN EN LA DIRECCIÓN NACIONAL DE CORREOS DEL PARAGUAY- DINACOPA.

Que, de acuerdo a la Ley Nro. 4016/2010, en su Capítulo III, Artículo 07 "Funciones", Inc. i) planificar y formular la política general de la DINACOPA, para el área comercial, operativa, administrativa y financiera"; y en el "Inc. j) diseñar, elaborar y proponer la normativa orgánica de la DINACOPA, para el mejor servicio y funcionamiento administrativo y operativo".-

Que, en fecha 19 de mayo de 2023, se dictó la Resolución Nº 938/2023/DG/SG, "POR LA CUAL SE DESIGNA ENCARGADO DE DESPACHO DE LA SECRETARÍA GENERAL, DE LA DIRECCIÓN NACIONAL DE CORREOS DEL PARAGUAY (DINACOPA)".-

Que, el Decreto Nº32 de fecha 15 de agosto del 2018 de la Presidencia de la República del Paraguay, nombra al Abg. LUIS FERNANDO SERVIN COLMAN, como Director General de la Dirección Nacional de Correos del Paraguay.-

EL DIRECTOR GENERAL DE LA DINACOPA

RESUELVE:

***Art 1°: APROBAR** la Política de Seguridad de la Información, de la Dirección Nacional de Correos del Paraguay - DINACOPA, conforme el "Anexo I", adjunto a la presente Resolución. –*

***Art 2°: DISPONER** que por intermedio de la Asesoría de Comunicación, se proceda a la difusión y socialización correspondiente.-*

***Art. 3°: COMUNICAR**, a quienes corresponda, cumplido, archivar.-*

.....

Lic. FERNANDO J. RIVEROS RAMOS
Encargado de Despacho
Secretaría General

.....

Abg. LUIS FERNANDO SERVIN COLMAN
Director General
Dirección Nacional de Correos del Paraguay
Dinacopa.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Dirección Nacional de Correos del Paraguay- DINACOPA

Elaboración:

Coordinación Mecip-Departamento Mejora Continua: Sra. Monique Mireya Mora; Funcionaria

Verificación:

Coordinación Mecip: Abg. Laritza Cardozo; Coordinadora
Dirección de Tecnología: Lic. Synthia Pereira, Directora

Aprobaciòn:

Comite de Control Interno; Comité Multidisciplinario-DINACOPA

Diseño y Diagramaciòn:

Sra. Monique Mireya Mora, Funcionaria

Dirección Nacional de Correos del Paraguay- DINACOPA
Dirección: 25 de Mayo esq. Yegros
Teléfono: (+595 21) 498112/13

www.correoparaguayo.gov.py

Asunción-Paraguay 2023

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

Luis Fernando Servín
Director General
DINACOPA

ÍNDICE

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

Abg. Lic. Fernando Servín
Director General
DINACOPA

INTRODUCCIÓN

Con la llegada del teletrabajo durante la pandemia y la conectividad que existe entre empresas y personas , resulta normal dejar de prestar la atención adecuada a la cantidad de correos electrónicos, llamadas o mensajes que se reciben a lo largo de una jornada laboral. Es entonces cuando entra en juego la ingeniería social y los ciberdelincuentes.

La elevada tasa de efectividad de estos ataques se debe a la fácil interacción entre atacante y usuario, así como la sofisticación de los engaños empleados para manipular y obtener la información confidencial que se busca.

En su mayoría, se sirven de técnicas de suplantación de identidad, por ejemplo, haciéndose pasar por un alto cargo, un proveedor o un compañero de la empresa, para poder mantener una conversación con la víctima. Valiéndose de esa relación de confianza, el ciberdelincuente solicita información de carácter sensible sobre la organización.

La seguridad de la información debe hacer frente a los riesgos, analizarlos, prevenirlos y encontrar soluciones rápidas para eliminarlos si se diera el caso.

La seguridad de la información y la ciberseguridad engloban un conjunto de técnicas y medidas para controlar todos los datos que se manejan dentro de una institución asegurando que no salgan del sistema establecido por la misma.

Este tipo de sistemas, principalmente se basan en las nuevas tecnologías, por tanto, la seguridad de la información resguardará los datos que están disponibles en dicho sistema y a los que solo tendrán acceso usuarios autorizados. Por otro lado, tampoco se podrán hacer modificaciones en la información a no ser que sea de la mano de los usuarios que tengan los permisos correspondientes.

La Política de Seguridad de la Información, tiene como objetivo establecer los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte a la mayoría de los procesos de negocio, actividades de servicios de la Dinacopa.

Abg. José Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

PRINCIPIOS

Datos como activos

Los datos del sector público son un activo del Estado y deben ser exactos, consistentes, oportunos, accesibles, completos, auditables y trazables.

OBJETIVOS

Los objetivos de la presente política están orientados a salvaguardar la seguridad de los activos (información y/o datos) respondiendo a tres cualidades principales:

-Crítica: es una pieza fundamental para que la Institución pueda llevar a cabo sus operaciones sin asumir demasiados riesgos.

-Valiosa: puesto que los datos que se manejan son esenciales, activo valioso para la Institución.

-Sensible: teniendo en cuenta que; al sistema solo podrán acceder las personas que estén debidamente autorizadas.

RESPONSABILIDADES

Las responsabilidades en la entidad, frente a la seguridad de la información y la ciberseguridad se encuentran jerárquicamente establecidas de la siguiente manera:

- La Alta Dirección, revisa y aprueba de forma periódica la eficacia, eficiencia y aplicabilidad de la política de acuerdo con la dinámica de la Institución.
- Seguridad de TIC conjuntamente con el Área de Seguridad de la Información, diseña y gestiona la política de seguridad de la información, ciberseguridad y las políticas relacionadas.

Abg. Luis Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

- Seguridad de TIC conjuntamente con el Área de Seguridad de la Información, revisa y evalúa la aplicación de procedimientos de seguridad de la información y controles de ciberseguridad para asegurar la adecuada ejecución de las políticas relacionadas.
- La seguridad de la información y la ciberseguridad son responsabilidades de todos y cada uno de los agentes involucrados como servidores públicos en la Entidad.
- Todo funcionario público debe reportar cualquier posible incidente cibernético de seguridad al Responsable de Seguridad de la Información (RSI), o, en su defecto, al Director de la UETIC de su Institución (Director de Tecnología). Es obligación de éstos reportar todo incidente cibernético de seguridad al CERT-PY enviando un correo electrónico a abuse@cert.gov.py, incluyendo una descripción del mismo, así como también cualquier dato que pueda ayudar a investigar el incidente, según sea el caso (logs, captura de pantalla, explicaciones, captura de tráficos, archivos, etc.).

RESOLUCIONES RELACIONADAS

La Política de Seguridad de la Información se encuentra sustentada mediante resoluciones emanadas por el MITIC, que tienen como propósito reglamentar el cumplimiento de la política de seguridad de la información y un análisis de información de consultas a varios textos de la seguridad de la información.

- RESOLUCIÓN MITIC N° 346-2020 – Reporte Obligatorio de Incidentes
- ISO 7498-2:1989 - Information processing systems
- RESOLUCIÓN MITIC N° 277-2020 – Guia de Controles Críticos de Ciberseguridad
- RESOLUCIÓN MITIC N° 733-2019 – Modelo de Gobernanza
- RESOLUCIÓN MITIC N° 699-2019 – Criterios de seguridad de software
- RESOLUCIÓN MITIC N° 218-2020 – Lineamientos del Portal Único de Gobierno y Trámites en Linea
- LEY Nº 5282/2014 LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL

Abg. Luis Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

RESPONSABILIDAD DE DATOS

Los datos del sector público tendrán una entidad pública responsable de su gestión y custodia durante todo el ciclo de vida, el cual es asignado según sus cometidos. Las entidades públicas que usen datos deberán respetar el contenido, no alterar la integridad ni la consistencia e informar de cualquier anomalía detectada.

PROTECCIÓN DE DATOS

Las entidades públicas deberán proteger los datos personales persiguiendo los siguientes principios:

- Legalidad.
- Veracidad.
- Finalidad.
- Seguridad de los datos.
- Reserva.
- Responsabilidad.

DIMENSIONES DE LA SEGURIDAD.

A fin de poder determinar el impacto que tendría en la Entidad un incidente que afectara a la seguridad de la información de los activos de información, y de poder establecer el nivel de criticidad, se tendrán en cuenta las siguientes dimensiones de la seguridad:

a) Integridad de la información: Garantiza la transmisión de los datos en un entorno seguro, utilizando protocolos seguros y técnicas para evitar posibles riesgos.

b)Confidencialidad de la información: Garantiza que solo las personas o entidades autorizadas tendrán acceso a la información y datos recopilados y que estos no se divulgarán sin el permiso de forma correspondiente.

Abg. Luis Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

c) Disponibilidad de la información: Accesibilidad a la información en todo momento para todas las personas o entidades autorizadas para su manejo y conocimiento.

d) Autenticación: capacidad de identificar al generador de la información, Por ejemplo: al recibir un mensaje de alguien, estar seguro de que es de ese alguien el que lo ha enviado, y no una tercera persona haciéndose pasar por otra (suplantación de identidad).

e) No Repudio: capacidad de demostrar o probar la participación de las partes (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, en una comunicación o en la realización de una determinada acción.

CRITERIOS DE CONFIDENCIALIDAD DE DOCUMENTOS

Los funcionarios de la Dinacopa deben dar cumplimiento a los lineamientos de seguridad de la información asociados a la clasificación, etiquetado y manejo de documentos e información y bases de datos personales, considerando los siguientes criterios de confidencialidad de documentos:

Sensible o confidencial: se entiende por datos sensibles aquellos que afectan la intimidad y/o seguridad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos o a misiones (viajes, etc.) de caracter riesgoso que les sean encomendadas siempre y cuando no contravenga con lo establecido en la Ley Nº 5282 /2014 LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL.

Abg. Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

Pública Interna: Se clasifica así la información que se publica y tiene impacto sobre los funcionarios de la Dinacopa. Documentos como; políticas, procedimientos, circulares, resoluciones, manuales y lineamientos, entre otros. siempre y cuando no se contrapongan a lo establecido en la Ley Nº 5282/2014 LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL.

Pública Externa: Se clasifica así la información que pueda interesar a cualquier ente o persona interna y externa. Teniendo en cuenta lo establecido en la Ley Nº 5282/2014 LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL , Art 8) establece como Regla general. Las fuentes públicas deben mantener actualizadas y a disposición del público en forma constante, como mínimo, las siguientes informaciones:

a) Su estructura orgánica;

b) Las facultades, deberes, funciones y/o atribuciones de sus órganos y dependencias internas;

c) Todo el marco normativo que rija su funcionamiento y las normas constitucionales, legales de alcance nacional o local y reglamentario cuya aplicación esté a su cargo;

d) Una descripción general de cómo funciona y cuál es el proceso de toma de decisiones;

e) El listado actualizado de todas las personas que cumplan una función pública o sean funcionarios públicos, con indicación de sus números de cédula de identidad civil, las funciones que realizan, los salarios u honorarios que perciben en forma mensual, incluyendo todos los adicionales, prestaciones complementarias y/o viáticos;

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

Fernando Servín
Director General
DINACOPA

f) Descripción de la política institucional y de los planes de acción;

g)Descripción de los programas institucionales en ejecución, con la definición de metas, el grado de ejecución de las mismas y el presupuesto aplicado a dichos programas, publicando trimestralmente informes de avance de resultados;

h) Informes de auditoría;

i) Informes de los viajes oficiales realizados dentro del territorio de la República o al extranjero;

j) Convenios y contratos celebrados, fecha de celebración, objeto, monto total de la contratación, plazos de ejecución, mecanismos de control y rendición de cuentas y, en su caso, estudios de impacto ambiental y/o planes de gestión ambiental;

k) Cartas oficiales;

l) Informes finales de consultorías;

m) Cuadros de resultados;

n) Lista de poderes vigentes otorgados a abogados;

o)Sistema de mantenimiento, clasificación e índice de los documentos existentes;

p)Descripción de los procedimientos previstos para que las personas interesadas puedan acceder a los documentos que obren en su poder, incluyendo el lugar en donde están archivados y el nombre del funcionario responsable; y,

q) Mecanismos de participación ciudadana.

Abg. Luis Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología

CUSTODIA DE DOCUMENTOS

El deber de diligencia y custodia durante la revisión o tramitación de los mismos.

En caso de compartir la información que está bajo su responsabilidad con otro proceso o colaborador de la Institución, el proceso solicitante deberá realizar dicha petición por medio escrito, correo electrónico, explicando la finalidad o bajo qué normativa lo solicita, a fin de garantizar el correcto manejo de la información.

CICLO DE VIDA DE LA INFORMACIÓN

La entidad deberá gestionar adecuadamente el ciclo de vida de la información, de manera que se puedan evitar usos incorrectos.

Captura: se produce la creación del dato en bruto. Un dato en bruto; es aquel que se obtiene a través de diferentes técnicas, métodos y herramientas de recolección de datos, se expresan de muchas formas, en formato JPG, PDF, Word, etc.

La Institución puede capturar o generar los datos de las siguientes formas:

Por Consumo: La Dinacopa en este caso consume los datos de otras entidades, por lo que los datos se producen de forma externa a la institución.

Por entrada: el servidor público de la institución es quien, de forma manual, consigue nuevos datos.

Por creación: los datos se capturan por dispositivos en distintos procesos empresariales.

Guardado:El dato en bruto es importante almacenar para protegerlo y garantizar su seguridad ante posibles ataques o errores informáticos, es recomendable implementar un proceso de recuperación (backup).

Abg. Luis Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

Dependiendo de si los datos son estructurados o no estructurados se almacenarán de dos posibles formas:

Estructurados: se denominan datos estructurados a aquellos que presentan un formato estandarizado, una estructura bien definida y que siguen un modelo de datos, siendo así accesibles tanto para los humanos, como para los programas. Estos datos habitualmente se guardan en las denominadas bases de datos relacionales. Estas permiten organizar los datos en tablas, haciendo que sean mucho más accesibles e identificables.

No estructurados: estos datos no tienen una arquitectura o estructura que se pueda identificar, por lo que no se ciñen a un modelo de datos ya definido. Por ello, no pueden estar en una base de datos relacional convencional, sino que deben almacenarse en una no relacional o NoSQL.

Utilización: Es recomendable que los diferentes equipos interesados tengan acceso a ellos a fin de que puedan participar en la toma de decisiones con argumentos sólidos.

Archivado: El archivo de datos consiste en copiar los datos en un espacio para su almacenamiento y, si es necesario, que puedan ser consultados de ser necesario.

Acceso a los documentos

El acceso a los documentos ha de realizarse exclusivamente por el funcionario autorizado por los responsables del tratamiento, siguiendo los mecanismos y procedimientos definidos.

El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas deberá ser reportado como un incidente de seguridad.

Abg. Luis Fernando Servín
General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

Entrada y salida de documentos o soportes

La entrada o salida de documentos y/o soportes debe registrarse indicando el tipo de documento o soporte, la fecha y hora, el emisor y/o receptor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable de la recepción o envío.

La entidad, debe proporcionar los medios o sistemas de información para realizar el registro de entrada y/o salida de los documentos o soportes.

BUENAS PRÁCTICAS CONTRA LA FUGA DE LA INFORMACIÓN

Se deberá asegurar la identificación, valoración y gestión de los activos y riesgos a través de un conjunto de buenas prácticas para la prevención de fugas de información. Especialmente se deberán tener en cuenta, al menos, los siguientes aspectos:

- Tomar precaución en el transporte y almacenamiento de la información, tener en cuenta que un incidente de fuga de información puede ser generado por un mal accionar de las personas y no sólo por una acción maliciosa.
- Uso adecuado de dispositivos extraíbles como USBs, CD/DVDs o similares a fin de evitar el riesgo de que acaben en manos inadecuadas mediante su pérdida o robo.
- Cifrar datos, crear contraseñas robustas y seguras, debe ser fácil de recordar y difícil de descifrar.
- Mantener la confidencialidad en todo momento, sopena de ser objeto de un sumario administrativo.
- En el uso de internet utilizar conexiones seguras, en caso de utilizar un equipo público para trabajar, no se debe acceder a archivos con información confidencial de forma local, a modo de evitar su disponibilidad y puedan ser visualizados por cualquier persona que utilice el mismo equipo en un futuro.

DIRECCIÓN NACIONAL DE CORREOS DINACOPA

rdo Servín
General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

- No compartir información con aquellos que no se puedan identificar, sea en persona o por teléfono. solicitar mayores detalles a fin de asegurar que son quienes dicen ser y ante la duda, no facilitar ningún dato. en su lugar, contactar a su superior inmediato.
- Uso del correo electrónico institucional diariamente.
- Poner especial atención en el tratamiento del correo electrónico, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, data leakage, etc.
- No abrir mensajes de correo de remitentes desconocidos, desconfíe de aquellos e-mails en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial.
- En caso de no reconocer al remitente, pasar el mouse por encima de su dirección de correo, a fin de visualizar el verdadero remitente, comprobar si la dirección está bien escrita, el dominio es de confianza y si corresponde con el nombre de quién envía el mail.
- Tener especial cuidado y atención a los correos o mensajes que soliciten hacer clic en un enlace, descargar archivos o responder con información, ya que podrían tratarse de intentos de phishing.
- Desconfiar de asuntos alarmistas, el asunto por lo general es llamativo ya que solicita alguna acción de manera urgente, ejemplo: "tiene un mensaje nuevo de seguridad", "detectados movimientos sospechosos", "eliminación de cuentas inactivas", "ha recibido una notificación", "tienes un paquete esperando", "ayúdanos con donaciones" etc.
- Atención en la redacción y ortografía; en algunos casos las frases suelen estar mal construidas o no tienen sentido, palabras con símbolos o caracteres extraños, faltas ortográficas, etc.
- Atención a los signos de personalización; los mensajes que se utilizan en la ingeniería social están poco o nada personalizados. ejemplos: "estimado cliente", "notificación a usuario" o "querido amigo", son indicios que deben llamar la atención.

Lic. Luis Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

- Impresión de documentación solo lo necesario.
- Salida de documentación, se diligencia el registro de control de salidas en el cual se relaciona los documentos requeridos, el cual contiene la siguiente información: a quien va dirigido y quien retira la información. Se sella y se recubre con un sobre de manila, por medio de correo electrónico informa al destinatario que información se le ha enviado y éste lo confirma.
- Los traslados de hardware de una dependencia a otra o las bajas de las mismas deberán ser informadas al departamento de Patrimonio dependiente de la Dirección de Administración y Finanzas, no así a la Dirección de Tecnología, teniendo en cuenta que ésta última es la encargada de la verificación para su posterior baja.
- Las salidas de equipos informáticos de la institución deberán ser autorizadas por el Director de la dependencia donde figure el equipo, el documento de salida del equipo deberá ser presentado al personal de seguridad postal o personal policial que custodia el edificio.
- Correcto uso de dispositivos móviles.
- Se deberá crear grupos de trabajos en el correo institucional, con el fin de que la información y/o requerimiento llegue a todos los funcionarios dentro de sus respectivas áreas (incluir el correo institucional de los funcionarios de la respectiva área y el correo institucional del dpto., dirección, auditoria, coordinación).

Cumplimiento

Se recuerda la necesidad del cumplimiento del marco normativo y de todo requisito de seguridad que en él esté implícito. La entidad tenderá a optimizar esta efectividad a través del recurso de una auditoría sobre las infraestructuras y las aplicaciones.

Abg. Luis Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA

Cumplimiento de los requisitos legales. Garantía de control sobre cualquier violación de las disposiciones legales vigentes, los contratos o los requisitos de seguridad de la información. Se considerará que el diseño, la operación, el uso y la gestión de los sistemas de información pueden estar sujetos a requisitos de seguridad. No olvidar que es responsabilidad de todas las áreas de la institución el conocimiento de la legislación y políticas vigentes.

REVISIÓN DE LA POLÍTICA

La aprobación de esta Política implica que su implantación contará con el apoyo de la Máxima Autoridad Institucional a fin de lograr todos los objetivos establecidos en la misma, como también cumplir con todos sus requisitos.

La presente Política de Seguridad de la Información, será revisada y aprobada anualmente. No obstante, si tuvieran lugar cambios relevantes en la sociedad o se identificaran cambios significativos en el entorno de amenazas y riesgos, ya sean estos de tipo operativo, legal, regulatorio o contractual, se procederá a su revisión siempre que se considere necesario, asegurando así, que la Política permanezca adaptada y adecuada en todo momento a la realidad institucional.

Abg. Luis Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

GLOSARIO

Incidentes cibernéticos: Un incidente cibernético de seguridad es una amenaza inminente a las políticas de seguridad de la información de una Institución, o cualquier hecho que comprometa la seguridad de la información de un sistema (confidencialidad, integridad o disponibilidad).

Almacenamiento: Es un conjunto de componentes electrónicos habilitados para leer o grabar datos en el soporte de almacenamiento de datos de forma temporal o permanente.

Cifrar datos: es el proceso de codificación de la información.

Contraseñas robustas: deben estar compuesta por números, símbolos y una combinación de letras mayúsculas y minúsculas

Sumario administrativo: tiene por finalidad la averiguaciòn o determinaciòn de la existencia de hechos y actos irregulares o ilicitos en el ejercicio de la funciòn pùblica

Forma local o archivos locales: son aquellos que se encuentran alojados en el propio dispositivo ya sea un móvil, PC, servidor

Correo electrónico: correo electrónico o e-mail es un servicio en linea que, al igual que ocurre con el correo postal tradicional, nos permite enviar y recibir mensajes a través de un servicio de red a múltiples destinatarios.

Phishing: es una técnica de la ingeniería social, consiste en el envío de correos electrónicos que suplantan la identidad de compañías u organismos públicos y solicitan información personal y bancaria al usuario

Ingeniería Social: Se llama ingeniería social a las diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de los usuarios. Los ciberdelincuentes engañan a sus victimas haciéndose pasar por otra persona

Ciberseguridad: conjunto de procedimientos y herramientas que se implementan con el fin de proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)

Activos de información: recursos utilizados por un sistema de seguridad de la información para que la Institución funcione y consiga sus objetivos. Los mismos incluyen, pero no se limitan a: los archivos de la Entidad , ya sea en formato electrónico o no; los sistemas, cuentas, equipos y redes en los que se almacenan, procesan y/o transmite la información institucional, así como también el conocimiento específico acerca de estos activos

Disponibilidad: se refiere al acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran

Integridad: se refiere a la exactitud y fiabilidad de los datos (información), estos deben estar completos, sin variaciones.

Confidencialidad: se refiere al acceso a la información por parte únicamente de quienes estén autorizados.

Usuario: persona que utiliza una computadora o un servicio de red.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Servidor: conjunto de computadoras capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

***Fuga de Información o Data Leakage*:** Es una salida no controlada de información (intencionada o no intencionada) que provoca que la misma llegue a personas no autorizadas o que su propietario pierda el control sobre el acceso a la misma por parte de terceros.

Amenaza: Peligro que un agente amenaza pueda explotar una vulnerabilidad.

Riesgo: Probabilidad de que un agente amenaza explote una vulnerabilidad y el impacto asociado con el negocio.

TIC: Tecnología de la Información y Comunicación, conjunto de equipos, cables y medios técnicos que transportan los servicios de comunicaciones desde los puntos de interconexión de los diferentes servicios

Abg. Luis Fernando Servín
Director General
DINACOPA

Lic. Synthia Pereira
Directora de Tecnología
Correo Paraguayo (DINACOPA)