PRESIDENCIA DE LA REPÚBLICA DOMINICANA
CONSEJO NACIONAL DE DROGAS

DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN

PLAN DE SEGURIDAD FÍSICA Y TECNOLÓGICA

SANTO DOMINGO, R.D.
NOVIEMBRE - 2018

INDICE

Las Normas Básicas de Control Interno, tiene entre sus pautas apoyar el aspecto de previsión de desastres ante cualquier eventualidad en las instituciones del Estado Dominicano. Frente a este compromiso se elabora el Plan de Seguridad Física y Tecnológica sobre los activos de tecnología de la información, tanto para el Departamento de Tecnología de la Información, como para los usuarios. Contiene una serie de pautas a ejecutar ante un eventual problema ya sea de índole catastrófica o un problema más simple.

Será ejecutado en lo referente a la parte de tecnología, por los Administradores de TIC, que desarrollan y ponen en práctica dichas medidas. El Plan contiene los pasos iniciales para las contingencias, medidas para los casos leves, medios y desastres graves, ha previsto también el protocolo típico a seguir ante eventualidades catastróficas y pautas para los usuarios o empleados.

El Consejo Nacional de Drogas junto a su Departamento de Tecnología de la Información pone en mano de todos los usuarios este documento que servirá de guía para la seguridad física y tecnológica a fin de recuperarnos ante cualquier eventualidad.

En la ciudad de Santo Domingo, Distrito Nacional, a los ocho (8) días del mes de noviembre del 2018.

LIC. RAFAEL GUERRERO PERALTA
Mayor General (R), P.N.
Presidente del Consejo Nacional de Drogas

Presidencia de la República Dominicana
Consejo Nacional de Drogas

CONSEJO NACIONAL DE DROGAS
REPÚBLICA DOMINICANA

DOCUMENTO ELABORADO POR:

Nombre y Apellido: Lic. Domingo García
Cargo: Encargado Departamento de Tecnología de la Información y Comunicación

Nombre y Apellido: Lic. Gracia Lourdes Guerrero
Cargo: Encargada División de Capacitación

Fecha: 05 noviembre, 2018

DISEÑO PORTADA:

Nombre y Apellido: Ing. Alex Oller

Cargo: Soporte Técnico

DOCUMENTO REVISADO POR:

Nombre y Apellido: Lic. Germania Melo
Cargo: Encargada Departamento de Planificación y Desarrollo

Fecha: 07 noviembre, 2018

DOCUMENTO APROBADO POR:

Nombre y Apellido: Lic. Rafael Guerrero Peralta
Cargo: Presidente Consejo Nacional de Drogas

Firma: _____

Fecha: 08 noviembre, 2018

Consejo Nacional de Drogas

Este Plan de Seguridad Física y Tecnológica tiene como propósito servir de contingencia ante posibles desastres naturales o de cualquier índole. Dentro de las pautas a seguir están las siguientes:

Pasos iniciales de plan de contingencia ante desastres.

1. Elaborar inventario informático del que consta la institución. Switchs, routers, cableado, computadoras de escritorios, laptops, servidores, licencias softwares y demás hardware. Un listado centralizado y actualizado ante cada nueva compra, actualización o pérdida por rotura.

Entre dicho listado ha de contemplar elementos de respaldo para caso de falla de los sistemas principales. Desde routers, SAIs (Sistemas de Alimentación Ininterrumpida), ratones, teclados, cableado, discos duros extraíbles, etc.

Normalmente la gestión de este inventariado basta con una Excel o Base de Datos aunque en redes más complejas se usan ERP o sistemas de gestión de recursos especializados.

2. En la parte referente al software, el Administrador deberá guardar con cuidado la configuración establecida tanto a nivel de red, intranet y extranet, VPNs, como las contraseñas pertinentes.
3. Configuración de acceso a las aplicaciones o recursos tanto desde servidores como el acceso desde el exterior de las oficinas.
4. Ejecución del Plan de contingencia de sistemas informáticos.

Plan básico ante medidas de importancia leve:

1. Cortes de conexiones locales de internet o electricidad. Aquí el protocolo va desde comprobar la conexión de los cables hasta solicitar soporte informático al servicio que tengan contratado la institución, si no dispusiese ya del mismo. Siempre que no sea un corte a nivel general este tipo de situaciones se soluciona rápido.

Plan de recuperación de desastres (medio):

1. Cortes o mal funcionamiento de la red inalámbrica. La rotura o desconexión de un switch provoca que internet deje de funcionar en una oficina, en estos casos la actuación es clara aquí, ir al concentrador y comprobar conexión, cableado, reinicio y sustitución de por repuesto lo antes posible.
2. A su vez disponer de alternativas como por ejemplo otro router que sirva Wifi por ejemplo, por esta razón se debe disponer de redundancia en la conectividad permitiendo más seguridad y estar siempre online.

Plan de recuperación ante desastres graves:

1. Actuación ante virus informáticos, desde individuales y locales hasta ransomwares. De estos últimos, los más peligrosos en la actualidad para una institución. Lanzar un protocolo de corte para evitar su propagación e infección.
2. Evaluar los daños y recuperación a través de backups.
3. Ante robos de información por hackers o empleados, investigar el origen de la fuga, consecuencias y cierre o paliación.
4. Medida urgente es cambiar la contraseña y analizar si hay vulnerabilidad subyacente y corregirla.

Desastres físicos naturales.

El protocolo típico a seguir ante eventualidades catastróficas de índole natural, en caso de que la institución se vea afectada por destrucción física de sus instalaciones, suele ser el traslado a otra sede (si la institución de otra), o trabajo remoto desde casa.

Sabotajes a lo interno de la institución. El enemigo en casa suele ser muy habitual, desde empleado descontento o espionaje. Una buena previsión de registrar el acceso a la información y su flujo ayudan a encontrar culpables.

1. Evitarlo es lo principal, pero si ocurre, esos informes de acceso ayudan a identificar al enemigo desleal y ayudar a la justicia para perseguir hechos delictivos.
2. Como sistemas de bloqueo para responder ante posibles ataques o intrusiones maliciosas a nuestra red, contamos con la facilidades de los siguientes sistemas de seguridad: Open DNS, anti malware, AVG antivirus

La educación y formación de los usuarios y empleados.

La mayoría de las veces de los hackeos a instituciones suelen venir de empleados internos que por negligencia o maldad han abierto puertas que deberían estar cerradas.

3. El personal será informado periódicamente sobre los planes de comunicación establecidos para que conozcan sus responsabilidades, métodos y así asegurar la calidad de las comunicaciones internas y externas.
4. Capacitar a empleados sobre la protección de la información y formas de trabajar: Cultura y prevención ante ataques de ingeniería social, de metodologías de seguridad básicas en el trabajo diario:

Políticas ante uso de redes sociales y lo que se comparte.

El correo electrónico:

- Usarlo correctamente para no caer en la duplicidad y compartir información sin control.
- Medios externos tipo USB o discos duros externos, control de instalación programas ajenos a la empresa.
- Viajes sobre conexiones inalámbricas y como proteger las comunicaciones.
- Protección de contraseñas y renovaciones periódicas.
- Encriptación de ordenadores para casos de pérdidas. Ej. con bitlocker
- Gestión de cambios de ordenadores. Al cambiar de ordenador se debe hacer un borrado real concienzudo de discos duros para evitar fugas de información.

Copias de seguridad Backups.

Sin duda las copias de seguridad ocupan un factor decisivo en cualquier plan de contingencia. Cuando falla la prevención actúa el respaldo.

- La frecuencia de los backups implica la capacidad de recuperación en tiempo.
- Un backup diario implica mucho gasto de hardware y recursos.

Desastres físicos naturales.

El protocolo típico a seguir ante eventualidades catastróficas de índole natural, en caso de que la institución se vea afectada por destrucción física de sus instalaciones, suele ser el traslado a otra sede (si la institución de otra), o trabajo remoto desde casa.

Sabotajes a lo interno de la institución. El enemigo en casa suele ser muy habitual, desde empleado descontento o espionaje. Una buena previsión de registrar el acceso a la información y su flujo ayudan a encontrar culpables.

1. Evitarlo es lo principal, pero si ocurre, esos informes de acceso ayudan a identificar al enemigo desleal y ayudar a la justicia para perseguir hechos delictivos.
2. Como sistemas de bloqueo para responder ante posibles ataques o intrusiones maliciosas a nuestra red, contamos con la facilidades de los siguientes sistemas de seguridad: Open DNS, anti malware, AVG antivirus

La educación y formación de los usuarios y empleados.

La mayoría de las veces de los hackeos a instituciones suelen venir de empleados internos que por negligencia o maldad han abierto puertas que deberían estar cerradas.

3. El personal será informado periódicamente sobre los planes de comunicación establecidos para que conozcan sus responsabilidades, métodos y así asegurar la calidad de las comunicaciones internas y externas.
4. Capacitar a empleados sobre la protección de la información y formas de trabajar: Cultura y prevención ante ataques de ingeniería social, de metodologías de seguridad básicas en el trabajo diario:

Políticas ante uso de redes sociales y lo que se comparte.

El correo electrónico:

- Usarlo correctamente para no caer en la duplicidad y compartir información sin control.
- Medios externos tipo USB o discos duros externos, control de instalación programas ajenos a la empresa.
- Viajes sobre conexiones inalámbricas y como proteger las comunicaciones.
- Protección de contraseñas y renovaciones periódicas.
- Encriptación de ordenadores para casos de pérdidas. Ej. con bitlocker
- Gestión de cambios de ordenadores. Al cambiar de ordenador se debe hacer un borrado real concienzudo de discos duros para evitar fugas de información.

Copias de seguridad Backups.

Sin duda las copias de seguridad ocupan un factor decisivo en cualquier plan de contingencia. Cuando falla la prevención actúa el respaldo.

- La frecuencia de los backups implica la capacidad de recuperación en tiempo.
- Un backup diario implica mucho gasto de hardware y recursos.

- Con la nube, ya no son necesarios backups utilizando los recursos físicos debido a la seguridad y control que ofrece un servicio en la nube, aunque no se deben descartar de plano.
- La calidad de los backups. Hay que probarlos como medida de seguridad restaurando cada cierto tiempo en un entorno de prueba y validando que la información está bien.
- Localización de las copias de seguridad es fundamental también que en la medida de lo posible esté lo más alejado de la localización original. Es fácil de entender que ante un incendio o terremoto, la copia de seguridad debería estar en otro edificio o país.

Plan de recuperación de desastres desde la perspectiva de la nube.

Una institucion gestionada desde la nube implica numerosas ventajas con respecto a la recuperación de desastres.

De hecho es una de sus principales cualidades además de la presencia y seguridad implícita de estos sistemas.

- Los virus. Un software en la nube como Dataprius, es inmune a virus del tipo Ransomware. No se puede encriptar algo a lo que el virus no puede acceder.
- Desastres naturales. Un terremoto que arrase una oficina no dejará la información de la institución en nada.
- Los miembros de la empresa siempre podrá acceder desde cualquier otro lugar, sede, oficina, casa, bar de la esquina y podrían reperarse de tan trágico suceso enseguida.
- Los backups. Trabajar en la nube, con mecanismos que evitan pérdidas como la redundancia, la papelera de reciclaje donde solo el administrador puede borrar evitan con mucho la necesidad de backups.
- Un backup de nube a nube es algo inmediato y transparente al usuario. Un click de ratón o simplemente automático. El acceso desde otra ubicación geográfica permite que el Administrador IT accesa a las copias por un camino, sino que además hay más. Todo esto de forma segura y controlada.

- Robos de información. Con la nube, el acceso a cada elemento almacenado queda registrado y es posible consultarlo, filtrarlo por fechas con una simple ventana y un botón. Algo que tradicionalmente requería un complejo sistema de servidor y configuración de ACL, ahora está de base en la nube. Cualquier acceso es registrado.
  La parte débil de la nube sería la conectividad en caso de corte de internet. Sin embargo, al tener la ubicuidad, el acceso a archivos desde dispositivos móviles o con conexiones de internet alternativas es inmediato. Un corte como el ejemplo de más arriba, puede paliarse con el móvil o tablet en unos segundos mientras el Administrador de IT soluciona el problema general.

Los planes ante desastres son una constante en la vida de las instituciones. La nube presenta cualidades que mejoran la respuesta y facilitan la vida ante estas situaciones, simplifican la labor de los Administradores IT de forma asombrosa.

Ahorra costes y da a la institución más seguridad y son menos vulnerables a los males que pueden acontecer en el mundo.