INSTITUTO NACIONAL DE CIBERSEGURIDAD

Decálogo de ciberseguridad para graduados sociales

1. **Diseña e implementa una política de seguridad de la información.**

   Es muy importante definir, documentar y difundir una política de seguridad que demuestre el compromiso del despacho con la seguridad, así como el desarrollo de normativas que recojan las obligaciones a las que están sujetos los graduados sociales en lo que respecta al tratamiento y seguridad de la información que maneja por razón de su actividad. Como por ejemplo: uso del equipo, uso de dispositivos o sistemas de almacenamiento externo, mesas limpias, teletrabajo, uso de dispositivos móviles, uso del correo electrónico, etc.

   Elabora políticas de seguridad para saber cómo va a abordar tu despacho la ciberseguridad.

2. **Establece controles eficaces para el acceso lógico a tus sistemas**.

   Algo tan sencillo como disponer de una política de contraseñas robusta para el acceso al sistema operativo y a las aplicaciones corporativas, nos servirá para evitar accesos no autorizados a la información que gestionan los graduados sociales. Debemos tener en cuenta aspectos como la longitud de las contraseñas, la obligación de cambio periódico, un bloqueo de la cuenta por intentos de acceso fallidos, etc.

   Cada vez es mayor la oferta de soluciones dirigidas a la protección de la información, que incluyen tanto productos que permiten el cifrado de la información como mecanismos de identificación y autenticación seguros. La elección de una solución u otra no es excluyente y cada despacho debe valorar la conveniencia de su implantación.

   Es importante inventariar la información que maneja el despacho y solo dar los permisos de acceso imprescindibles para los usuarios que realmente la necesiten

3. **Realiza periódicamente copias de seguridad.**

   La pérdida de información es una amenaza real para el graduado social, que se puede limitar en gran medida realizando copias de seguridad periódicas. Es recomendable hacer –como mínimo- una copia semanalmente de la información más importante y verificar periódicamente que podemos restaurarla y recuperar los datos correctamente. Además, es aconsejable que la copia de seguridad la mantengamos en un soporte distinto al que alberga los datos originales.

La información es el activo más importante del despacho. Garantiza su disponibilidad realizando periódicamente copias de seguridad, empleando los métodos y soportes más adecuados para ello.

4. **Protege a tu despacho y a tus clientes frente a malware.**

   Una de las principales amenazas a las que se encuentra expuesto cualquier despacho de graduados sociales es la infección de sus equipos por virus. Para esto, la mejor medida es disponer de un antivirus siempre actualizado y debidamente configurado, tanto en los equipos personales como en los servidores.

   Instala software antimalware en todos los dispositivos del despacho, e implanta otras medidas especiales, como diseñar su red de forma segura o bastionar adecuadamente otros elementos claves, como pueden ser las cuentas de administración.

5. **Actualiza los sistemas.**

   A diario se descubren numerosas vulnerabilidades que ponen en riesgo nuestra información. Estas no suponen un peligro siempre y cuando mantengamos una política de actualizaciones automatizadas que permitan tener todos nuestros sistemas con los últimos parches de seguridad aplicables. Si no fuera posible, lo más conveniente es definir, documentar e implantar un procedimiento para la gestión de vulnerabilidades que incluya tanto la revisión periódica como las comunicaciones, requisitos y aspectos a tener en cuenta para el despliegue de las actualizaciones de seguridad que las corrigen.

   La correcta actualización de los sistemas garantiza un rendimiento óptimo y seguro de todas las aplicaciones y dispositivos del despacho.

6. **Controla la seguridad de la red del despacho.**

   Desde el mismo momento en que la información del despacho está almacenada en equipos y dispositivos conectados a internet, se encuentra expuesta a riesgos que pueden hacer que sea accesible desde el exterior. Por ello, debemos implementar medidas de seguridad que protejan estos accesos, como es el caso del firewall. Además, si nuestro despacho dispone de redes Wifi, deberemos configurarlas a través de protocolos seguros.

   Debemos restringir y controlar al máximo el acceso externo a la red corporativa, y poner especial vigilancia en el uso de dispositivos de almacenamiento extraíbles.

7. **Medidas de seguridad para la transmisión de información.**

   Atrás queda cuando enviábamos nuestra información en CD, DVD o dispositivos de almacenamiento USB. Ahora la mayor parte de información la compartimos a través de internet y de la nube. Por eso debemos proteger todos los canales por los que compartimos información sensible de nuestra organización. ¿Cómo podemos hacerlo? El cifrado es una solución eficaz.

   Protege la información en tránsito para garantizar la seguridad de la información que sale de las instalaciones del despacho.

8. **Gestión de soportes.**

   Los soportes extraíbles constituyen una de los principales amenazas de fuga de información, así como de infección por malware. Evalúa la posibilidad de bloquear estos puertos y eliminar las unidades lectoras/grabadoras de soportes ópticos de los equipos de los usuarios.

   Adicionalmente al cifrado de la información, conviene diseñar un procedimiento de almacenamiento y borrado seguro de la información que contengan los soportes que vayan a retirarse.

   Utiliza los tipos de soporte de almacenamiento adecuados a tu despacho para garantizar la correcta disponibilidad de la información del despacho, considerando aspectos tales como la capacidad, la tasa de transferencia, etc. de cada uno de ellos. Y cifra la información ahí almacenada.

9. **Registro de actividad.**

   Habilitar registros de actividad para el acceso a la información del despacho permite la trazabilidad de todas las acciones llevadas a cabo sobre aquella (arranque de sistemas, accesos, borrados, etc.). En caso de incidente, esta información será esencial para conocer una serie de datos que servirán para la posterior investigación, y también nos permitirá prever, identificar y gestionar amenazas para la información que almacenamos en nuestro despacho.

   Implementa un registro de actividad en tus sistemas que permita recabar los detalles relevantes referidos a los eventos más trascendentes en los sistemas de información.

10. **Continuidad de negocio.**

    Conviene preguntarse cómo actuaremos el día en que suframos un incidente de seguridad, y desarrollar un plan de continuidad de negocio adecuado, que deberemos procedimentar para que, llegado el caso, tengamos claros los pasos a dar de cara a volver a la normalidad lo antes posible. Eso incluye planificar acciones de continuidad

que confirmen que los planes están debidamente actualizados y, lo más importante, que son eficaces.

Es imprescindible que definamos y probemos un conjunto de tareas y acciones orientadas a recuperar cuanto antes la actividad normal del despacho ante la aparición de un incidente de seguridad.

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Buenas prácticas en ciberseguridad para graduados sociales

- Instala un antivirus y un cortafuegos y mantenlos actualizados.
- Mantén tu equipo constantemente actualizado y protegido con contraseña segura.
- Nunca ejecutes programas o ficheros de dudoso origen, ni sigas un enlace que te llegue por correo y que te parezca extraño.
- Protege la información con herramientas de cifrado.
- No conectes a tu equipo un USB cuya procedencia ignoras.
- Utiliza el sentido común. Sé precavido ante cualquier cosa que te parezca sospechosa.
- La información es clave para identificar los riesgos y poder combatirlos. Procura estar al día de las amenazas que circulan.
- Conciencia a tus empleados en buenas prácticas en ciberseguridad.
- Haz siempre copias de seguridad.
- En caso de sufrir un incidente de ciberseguridad, contacto de inmediato con el CERT de INCIBE.