BOLETÍN

Revista profesional de la
Asociación de Calidad en Salud de Puerto Rico

Octubre 2019

Junta de Oficiales 2019-2020

Presidenta
Miressa Rivera, MHSA

Presidenta Electa
Katia León, MPH

Pasada Presidenta
Katheryn S. López Sánchez, MHSA

Vicepresidenta
Zivany García, MPH

Secretaria
Ana Y Antongioirgi Cruz, RN, MSN

Tesorera
Lillian Zamora, MA

Vocales
Itza Soto, MSN
Mónica Torres, MBA
Sandra Díaz, RN, MSN, CPUM
Verónica Merced, BHS, MPH

Saludos cordiales,

Comenzamos otro año lleno de retos en la industria de la salud. La Junta de Oficiales 2019-2020 refuerza su compromiso con la educación de los profesionales de la salud con varias actividades educativas durante el año.

Nuestro objetivo sigue siendo proveer herramientas para nuestros compañeros, de manera que se provean servicios de alta calidad para nuestros pacientes. Les invitamos a participar de las actividad que ACESA tiene para ustedes.

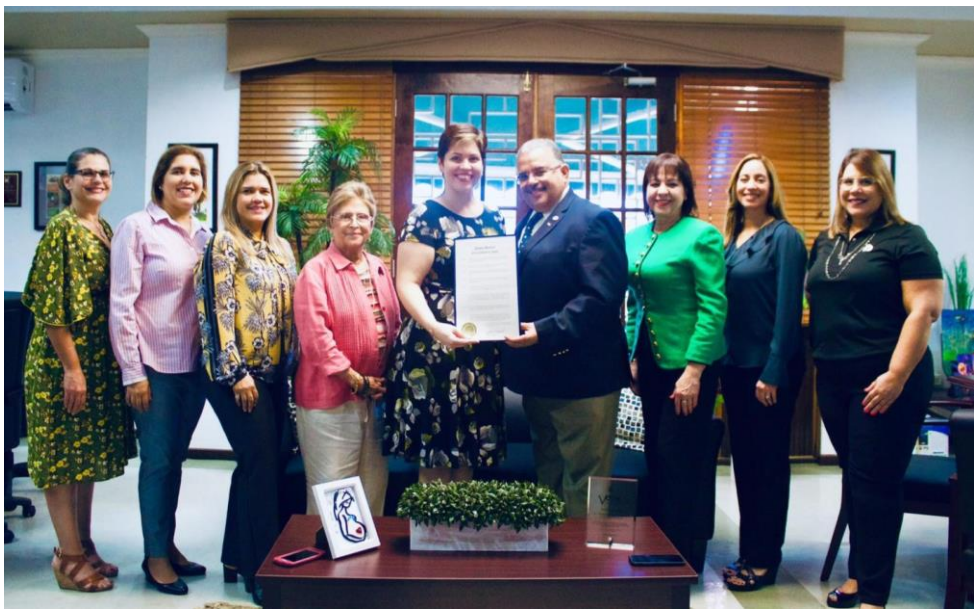
¡Espero saludarles pronto!

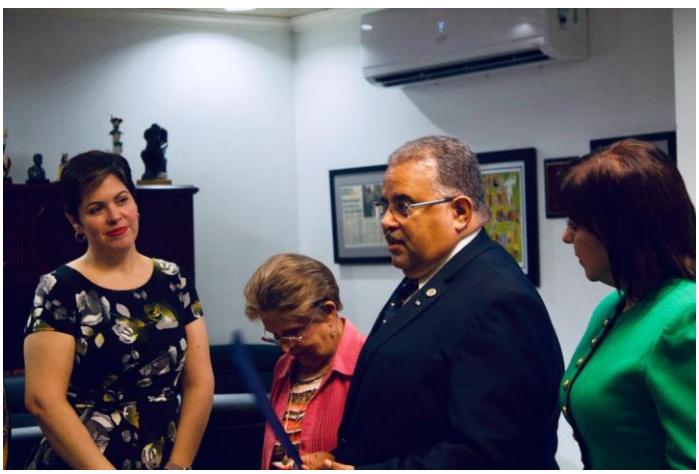
Miressa Rivera, MHSA
Presidenta

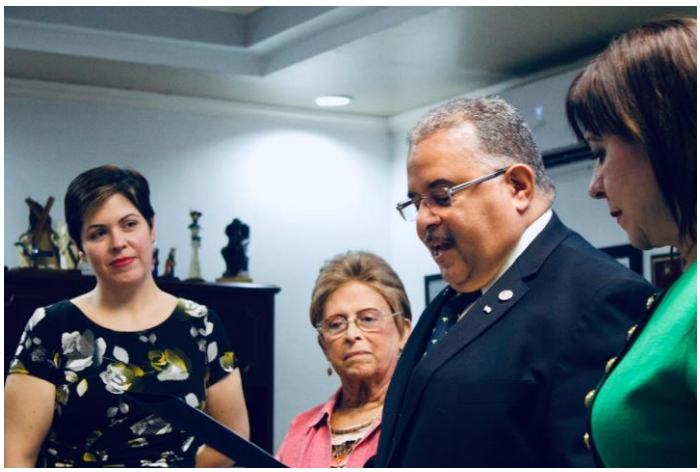
Contenido

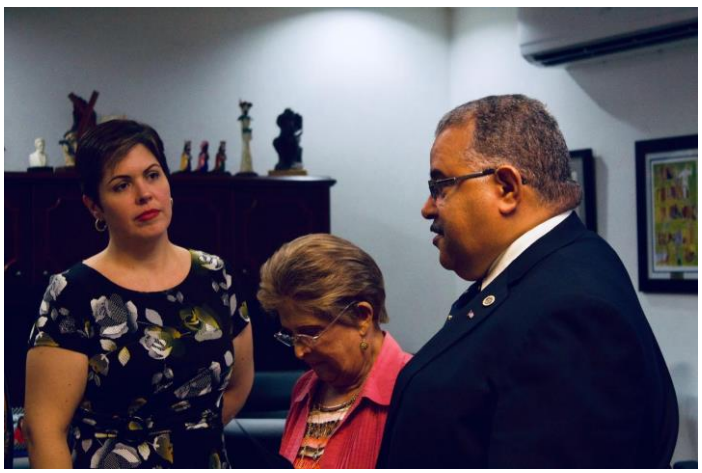
Entrega de la Proclama de la Calidad

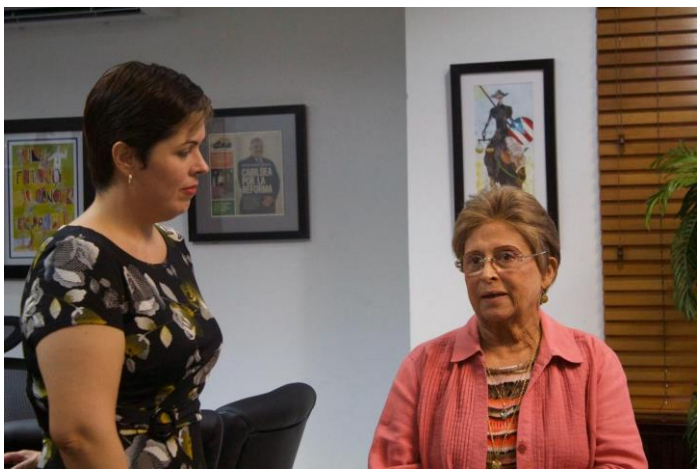
El pasado miércoles, 9 de octubre representantes de la Junta de Oficiales de la Asociación recibió por parte del Secretario del Departamento de Salud, Hon. Rafael Rodríguez Mercado, MD/FAANS, FACS la proclama de la Semana Nacional de la Calidad en Salud. Invitamos a todos nuestros Socios a realizar actividades en sus instituciones en celebración de la Semana Nacional de la Calidad en Salud. Envíennos imágenes y detalles a acesa.socios@gmail.com para compartirlas en la próxima edición.

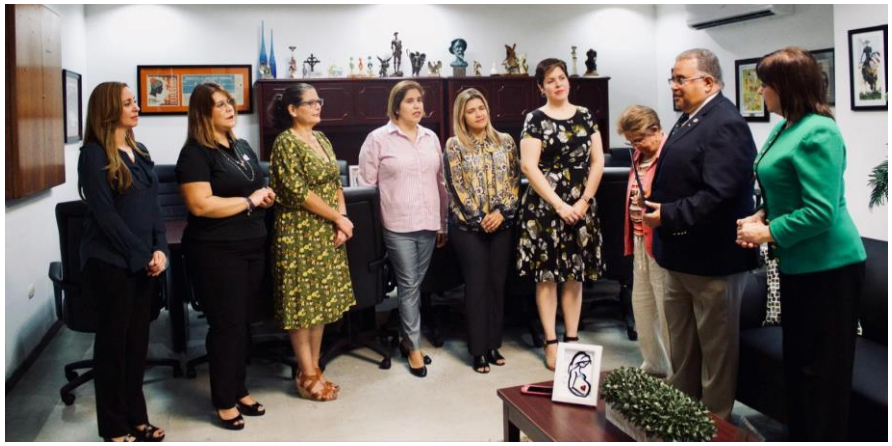


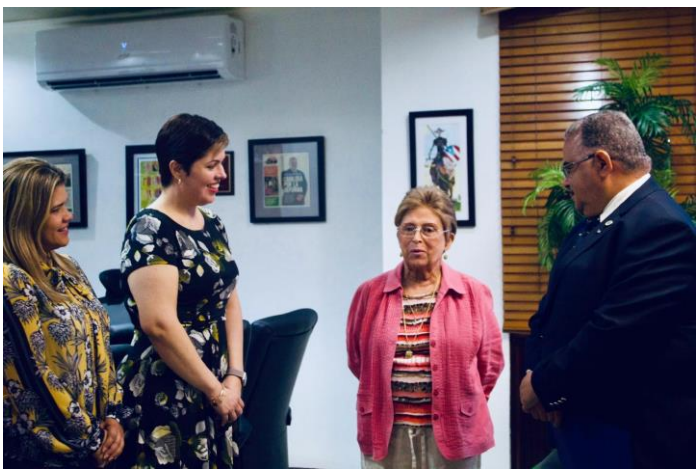


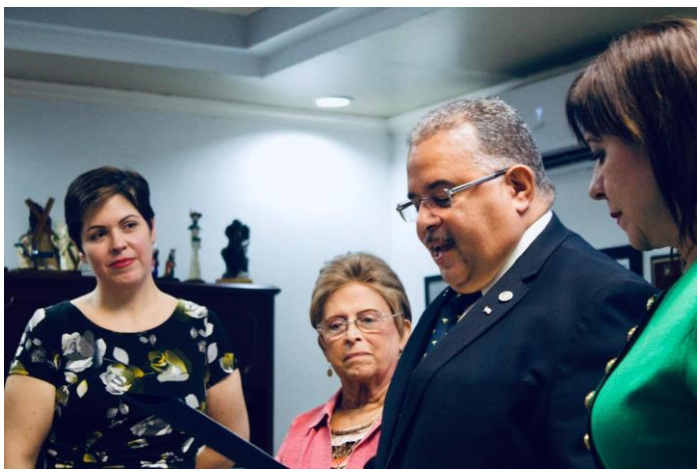


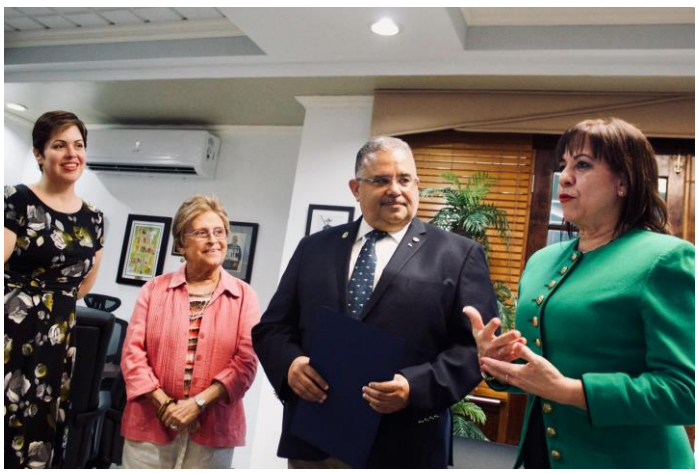


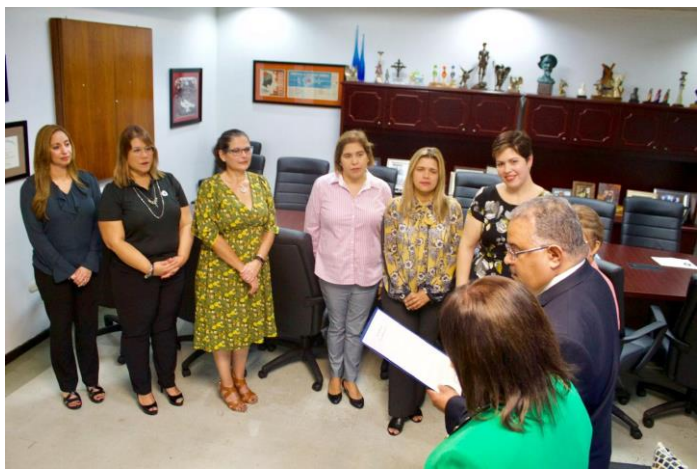


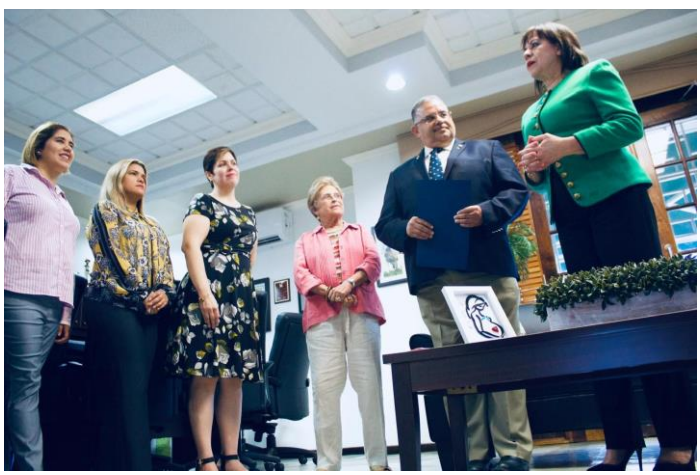


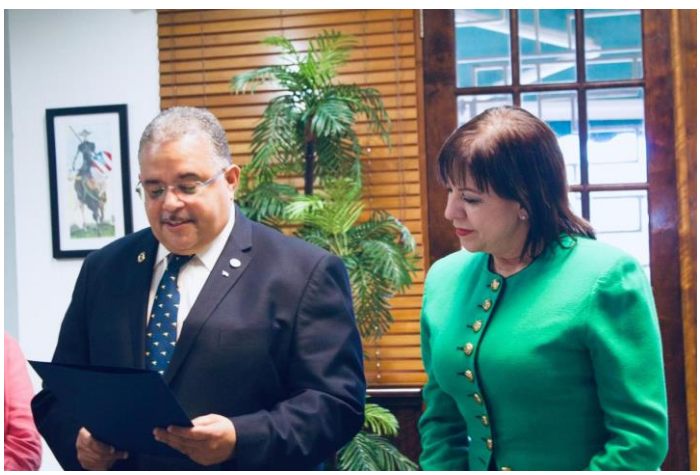












PROCLAMA DEL SECRETARIO DE SALUD

Semana Nacional de la Calidad en Salud

Por Cuanto: La Calidad de servicios se define como la actividad en la cual los servicios de salud se ofrecen de forma segura, efectiva, competente y eficiente para obtener los resultados deseados y la satisfacción plena de los pacientes y la población en general;

Por Cuanto: El concepto de calidad en los servicios de salud enfatiza las funciones, características y práctica de un servicio, que lo hace capaz de satisfacer las necesidades de sus usuarios;

Por Cuanto: El proceso de calidad y seguridad del paciente se fundamenta en actividades planificadas, integradas y con propósito, para estimar, vigilar y promover la excelencia y seguridad del cuidado o servicio que se provee;

Por Cuanto: La calidad y seguridad del paciente enfatiza el trabajo integrado, con la participación de los equipos de salud a todos los niveles, para la identificación y resolución de problemas, así como la implantación de medidas correctivas pertinentes;

Por Cuanto: El proceso de calidad de los servicios de salud y seguridad del paciente promueve el aumento en conocimientos, basado en evidencia científica y desarrollo de estrategias innovadoras para lograr exitosamente las diversas funciones en el desempeño organizacional;

Por Cuanto: La misión de las instituciones, que ofrecen servicios de salud, debe promover el mejoramiento continuo en el desempeño organizacional y la seseguridad de pacientel. El compromiso institucional con la calidad de servicios debe demostrarse a través de un programa de trabajo continuo, que refleje destrezas de planificación, diseño, medición, evaluación y mejoramiento de la calidad del servicio que se ofrece;

Por Cuanto: Se reconoce la responsabilidad y compromiso de cada profesional en las instituciones de salud, en particular a los profesionales que laboran en la implantación y mantenimiento de los programas de calidad para lograr el mejoramiento continuo del servicio;

Por Tanto: Yo, Rafael Rodríguez Mercado, Secretario del Departamento de Salud del Gobierno de Puerto Rico, y en virtud de la autoridad que me confiere la ley, proclamo el periodo de tiempo del 20 al 26 de octubre de 2019 como la **Semana Nacional de la Calidad en Salud.** Exhorto a todos los profesionales de la salud a continuar propiciando y fomentando el compromiso con la calidad y excelencia en los servicios de salud, un reto ineludible que es responsabilidad de todos los que integramos el sector de la salud.

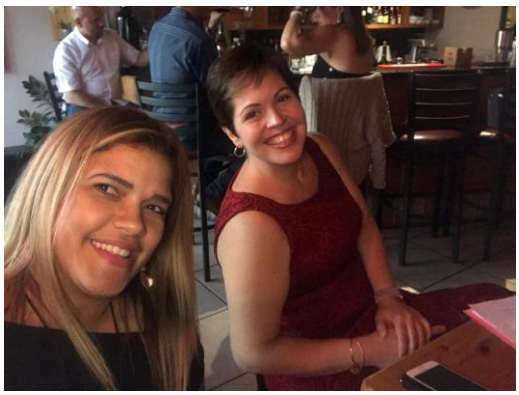
En testimonio de lo cual, firmo la presente y hago estampar el sello del Departamento de Salud en San Juan, Puerto Rico, hoy, 19 de octubre de 2019.

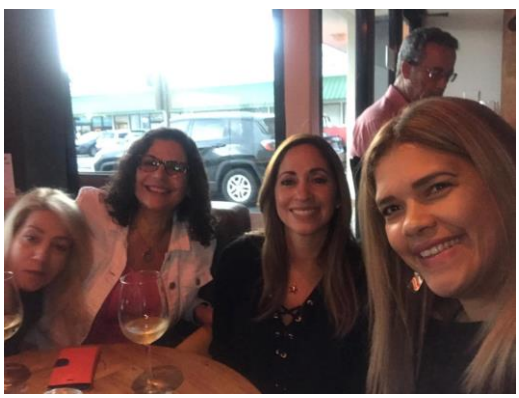
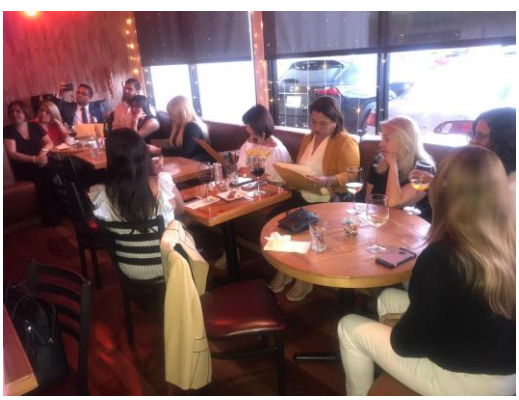
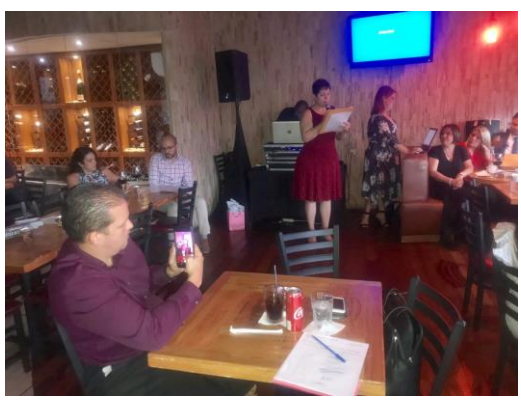
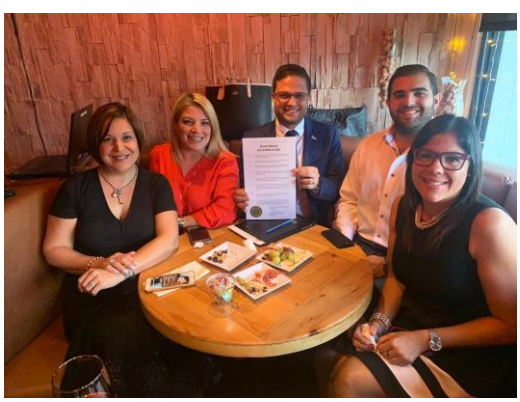
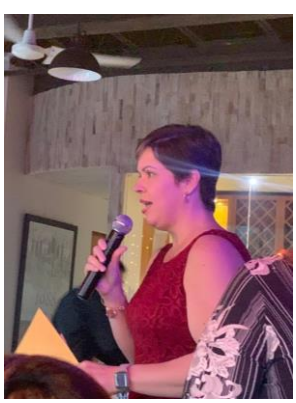
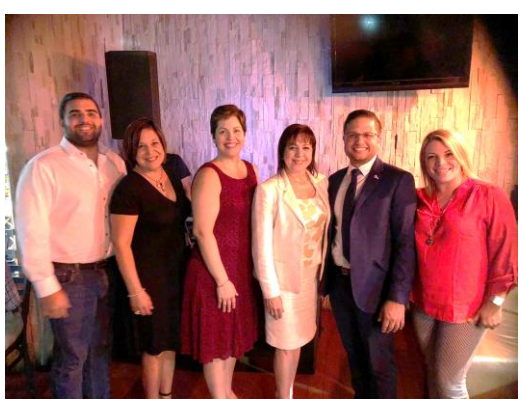
Rafael Rodríguez Mercado, MD, FAANS, FACS
Secretario
Departamento de Salud

Integrándonos en Calidad

El pasado viernes, 11 de octubre en Vínissimo, llevamos a cabo nuestra primera actividad de confraternización donde leímos la Proclama recibida por parte del Departamento de Salud que establece la Semana Nacional de Calidad en el Cuidado de Salud. Agradecemos a APS Healthcare que nos colaboró con la Lcda. Yaritza Castro, MSW como recurso de la la conferencia “Manejo de Emociones”. En la actividad, contamos con la presencia de representantes de hospitales, planes médicos y servicios de salud primaria. Pendiente a futuras actividades de *networking* para que participes, hagas importantes enlaces y pases un buen rato.





Seguridad en los Sistemas de Información

Resumen de Presentación realizada por Juan G Del Valle Vázquez , Information System Security Officer del Hospital Auxilio Mutuo

Nos encontramos en momentos cruciales en cuanto a los sistemas de información. Hoy día que cada persona tiene la tecnología al alcance de sus manos, literalmente, se incrementan las amenazas a nuestros sistemas, poniendo el riesgo tanto nuestra información personal como la de nuestros pacientes. Es importante realizar análisis de riesgo y realizar planes de acción para mitigar posibles daños y realizar planes correctivos de acuerdo a las vulnerabilidades identificadas.

Un programa de seguridad en los sistemas de información consiste de la integración de las normas y procedimientos de seguridad de información con las reglas del negocio en cuestión. Además, toda empresa debe implementar y documentar un programa de seguridad de sus sistemas de información. Por lo tanto, es fundamental que los ejecutivos de la empresa deben establecer establecerán cuál es la misión y los objetivos que el programa debe establecer para cumplir con las leyes y regulaciones estatales y federales que le apliquen.

Para esto, debe considerar dentro del Programa de Seguridad los siguiente:

- Inventario y documentación de los equipos y aplicaciones que estén conectados a la red.
- Realizar un análisis de riesgo para detectar las amenazas y vulnerabilidades
- Manejar los riesgos ya sean mitigando la amenaza o transfiriendo el riesgo a un ente externo.

Es importante que desarrolle un programa de manejo de incidentes para documentar todo lo relacionado a eventos de seguridad y cree un *Disaster Recovery Plan* (DRP), en caso de sufrir una pérdida de data ya sea por un ataque cibernético o eventos externos. En adición, debe implementar controles de seguridad en los sistemas, proveer adiestramiento a los empleados, realizar auditorías, entre otras.

Los *Malwares:*

"Malicious Software" se instalan en los equipos (computadoras, móviles, tablets) para tomar control y ganar así acceso al contenido de los mismos. Esto le permite espiar lo que usted hace en el Internet, robar las credenciales que tenga grabadas en sus equipos y robar archivos que tenga en su computadora. Además, atacan toda clase de sistemas operativos y dispositivos. Por ejemplo, Windows y Android son los más atacados por ser los de mayor popularidad

Virus: infectan archivos con el solo propósito de modificarlo o dañarlo.

Aquí algunos ejemplos:

- ILOVEYOU: Propagado en el año 2000 través de correos electrónicos, dejo sobre $10 billones en pérdidas y se cree que sobre el 10% de las computadoras en el mundo fueron infectadas.
- Melissa: Propagado en el año 1999 través de correos electrónicos. Causó sobre $80 millones en daños
- Sasser: Descubierto en el 2004. Atacó una vulnerabilidad en el sistema operativo Windows. Los daños fueron estimados en sobre $18 billones y sobre un millón de computadoras infectadas.

Backdoors: Es un programa que abre un puerta trasera en sistema operativo permitiendo que un atacante entre a su computadora sin que usted se percate. El atacante tendrá control total de su computadora, podrá ver todo lo que usted hace e incluso puede borrar sus archivos, copiarlos y hasta encender su webcam.

Botnet: Infectan todo tipo de equipos que estén conectados en el internet, como las computadoras, cámaras de seguridad, televisores (SmartTV), etc. La función de este malware es utilizar los equipos infectados y lanzar ataques simultáneos para afectar servicios, extraer información, entre otros. Un ejemplo reciente es el Botnet llamado Mirai que afecto cientos de equipos y paginas de Internet en todo el mundo.

Adware: Este tipo de malware abre ventanas de publicidad de diferentes productos o servicios.

Correo Electrónico (EMAIL)

Algo muy utilizado es el correo electrónico para enviar y recibir información. Recuerde que toda institución y usted como individuo debe proteger toda información confidencial, esto incluye el seguro social, la información de pacientes y la financiera. Entre las medidas de seguridad para proteger la información se encuentra el cifrado del correo electrónico y colocar una contraseña al documento. Evite abrir mensajes si no conoce al remitente o si conoce al remitente pero no acostumbra intercambiar mensajes. Recuerde, no haga clic en un enlace o descargue un archivo si no le es familiar. Si recibe un correo electrónico desconocido, repórtelo inmediatamente a su Departamento de Información y Tecnología ya que puede ser víctima de robo de su identidad o perder acceso a sus archivos y/o cuentas personales

Phishing

- El Phishing es un ataque empleado por ciber-criminales con el objetivo de engañar y hacer que la persona revele información personal o que realice ciertas acciones en su equipo.
- Estos ataques comienzan cuando un criminal envía un mensaje haciéndose pasar por una persona o una entidad que conoces como, por ejemplo, un amigo, tu banco, portales de video como Netflix, o una tienda online.
- Estos mensajes llegan con algún tipo de instrucciones para que entres a un link y entres tu información personal, ya sea tus credenciales de tu cuenta de banco o tus credenciales de tu cuenta de la tienda online como por ejemplo, Amazon o EBay.
- El contenido de los mensajes es bastante elaborado con el fin de que el mensaje se vea lo más cercano a un comunicado oficial de la tienda, banco, etc.
- Este tipo de ataque no se limita a mensajes de correos electrónicos, también se usan los programas de mensajería instantánea como Whatsapp o por las redes sociales.

Como evitar ser víctima de Phishing

- No haga clic en ningún enlace (link) que tenga el mensaje
- No descargue ningún archivo que incluya el mensaje
- Borre el mensaje
- Mantenga su sistema operativo con todas las actualizaciones al día
- Mantenga actualizado y activado su antivirus
- Esto debe de aplicarse a todos los equipos, incluyendo Apple, Android, Windows, Linux, etc.
- ¡¡¡Oriente a sus empleados!!!

Ransomware

- Tipo de malware que destruye documentos y archivos de la computadora.
- Infecta su computadora, encripta ciertos archivos o todo el disco duro, y le informa que debe de pagar una cantidad de dinero (usualmente en Bitcoins) para poder brindarle acceso a sus archivos.
- Se propaga a través de correos electrónicos, dispositivos de almacenamientos externos, etc.
- Ransomware “Bad Rabbit”
- Ransomware WannaCry

Algunas recomendaciones generales:

Contraseñas

- Nunca comparta las contraseñas o códigos con nadie.
- Cambie su contraseña si descubre sospecha que alguien la conoce.
- Nunca escriba sus contraseñas en papel, “post-it”, etc.
- Evite utilizar información que puedan saber de usted, como por ejemplo:
  - Fecha de nacimiento
  - Nombre de sus animales
  - Nombre de sus hijos o parientes cercanos
  - Cada usuario es el responsable de
  - lo que suceda con su cuenta
- No utilice las mismas contraseñas para sus cuentas del trabajo y las personales.
- No reúse contraseñas, por ejemplo:
  - Francia1
  - Francia2
- Cambie sus contraseñas cada 60 a 90 días.
- Trate de utilizar frases como una contraseña, como por ejemplo:
  - Mivi@jeenel2018fueestup3ndo
  - Mi@buelametirabaconlachanclet4
- Utilice contraseñas largas, complejas y únicas, como por ejemplo:
  - 9@kj*YbM25nGnl
  - Lq@6eNuQcwyMvW5C

Autenticación Multifactorial (MFA)

- Combina dos o más credenciales independientes
- lo que sabe el usuario (contraseña)
- lo que tiene el usuario (token de seguridad) y
- lo que es el usuario (verificación biométrica)

Protección de la Información

- Envíe información confidencial por correo electrónico de manera segura (encriptada).
- No abra correos electrónicos que usted no esperaba o le parezcan sospechosos.
- No imprima documentos con información confidencial si no hay la necesidad de hacerlo.
- No copie ningún archivo a algún medio de almacenamiento externo (Pendrive, disco duro externo, CD's, etc.)
- Evite navegar en páginas de Internet no relacionadas a sus funciones en horas de trabajo.
- No entre a ver información de pacientes que usted no tenga asignados.

Seguridad Física

- Asegure el espacio físico donde se maneja información confidencial.
- Cuestione la presencia de toda persona extraña en áreas restringidas como las unidades de enfermería, cuartos eléctricos, cuartos de comunicaciones.
- Alerte a su supervisor y/o seguridad.
- Asegúrese de que todo personal tenga su identificación.
- Todo personal contratista que va a realizar algún trabajo debe de tener su identificación de la compañía. El personal del Hospital se debe asegurar de que esa persona este autorizada a trabajar en el área.
- Siempre bloquee o saque su usuario de la computadora cuando se retira de la misma.
- No permita que otro usuario utilice su cuenta de usuario. Recuerde usted es el responsable de lo que suceda con su cuenta de usuario en el sistema.
- Nunca deje documentos con material confidencial desatendido.
- Tenga disponible las políticas y normas de uso del sistema en un lugar accesible y rápido de acceder como el intranet de su compañía.

Medidas de Prevención

- No deje ningún documento con información confidencial desatendido.
- Sea consciente del contenido cuando disponga de un documento.
- Siga las políticas y normas del uso del sistema y de Recursos Humanos.
- No permita que usen su cuenta de usuario. Usted es el responsable de lo que suceda con su cuenta.
- El que usted tenga acceso al sistema no le da derecho a acceder información de casos que no tenga asignados. Ejemplo: Usted pertenece a pediatría pero está navegando en cuentas de pacientes de Intensivo adulto.
- Sea precavido en abrir correos electrónicos de personas que no conoce o que no estaba esperando.
- No debe navegar por páginas de compras, banca, noticias, etc. en computadoras de la empresa si no está autorizado.
- No debe en enviar por mensajes de texto con información de pacientes.
- No debe usar dispositivos de almacenamientos como Pendrive, discos duros externos, teléfonos, etc.
- No debe de instalar aplicaciones que no estén autorizadas por el Departamento de Información y Tecnología.
- Utilice contraseñas seguras (vea sección de Contraseñas)
- No habilite la opción de "Remember Password" en las páginas de internet que visita
- No escriba sus credenciales en papeles o notas.
- No coloque información confidencial de la compañía o personal en las redes sociales.
- Utilice en la medida que sea posible autenticación multifactorial (MFA).

Contáctanos

https://www.acesapr.org/

Asociación de Calidad en Salud de Puerto Rico

acesa.socios@gmail.com

PO Box 367783 San Juan PR 00936-7783

787-400-4484

¡Hazte socio hoy!