CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

BUENAS PRÁCTICAS

Medidas de ciberseguridad en vacaciones

Introducción...

Antes de comenzar las vacaciones, prepara a tu organización o institución para mantener la seguridad informática para que puedas descansar y disfrutar tranquilamente.

Existen distintos aspectos que debes considerar en esta época. Por una parte, algunos de los trabajadores no estarán, pero también ingresarán nuevas personas a las que debes capacitar o configurar sus sistemas de forma segura.

En ciberseguridad debes considerar distintos ámbitos para prevenir y evitar un incidente.

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Correo electrónico

Por regla general, el correo electrónico institucional se debe utilizar solo para ejercer las funciones designadas de acuerdo al cargo. Por lo tanto, para promover el correcto uso de este canal, recomendamos:

- Identificar correctamente al usuario para que el destinatario pueda reconocer adecuadamente la identidad del remitente y el organismo de procedencia.
- En caso de configurar el correo electrónico en dispositivos móviles con conexión a Internet, implementa algún método de acceso o bloqueo del teléfono. Es mejor usar un pin numérico en vez de un patrón de puntos.
- Contar con protocolos en caso de robo o pérdida del dispositivo de un trabajador. Por ejemplo, cuándo bloquear, cambiar contraseñas y a quién notificar.
- Desactivar los accesos a las cuentas de correo cuando los trabajadores, sin importar el cargo, estén ausentes.
- Solicitar que se active la respuesta automática para notificar que la persona está ausente.
- Utilizar filtros antispam con un nivel alto para que los usuarios reciban la menor cantidad posible de correos no deseados con campañas de phishing y malware.

Para nuevas contrataciones...

Recuerda informar e implementar las medidas de seguridad de la organización para el uso correcto del correo electrónico.

VPN

Si bien el uso de una VPN permite el acceso confidencial a la información desde cualquier sitio para los trabajadores, de todas formas hay que ser cuidadosos a la hora de configurar y asignar este recurso.

- Antes de adquirir un servicio de VPN, infórmate sobre los protocolos y los tipos de cifrado para elegir la opción más segura.
- Elabora políticas de seguridad para los dispositivos y las conexiones remotas autorizadas.
- Mantén un control de acceso y asigna roles.
- Identifica a los usuarios, equipos, sistema operativo, navegadores y software que utilizan la VPN.
- Asegúrate que computadores personales y sin antivirus no se conecten a la VPN.
- Evita vulnerabilidades asegurándote de mantener los software y hardware de las máquinas de VPN actualizadas.

- Filtra el tráfico y monitorea las direcciones que utilizan la VPN. De esta forma, mejoramos la seguridad y ante un incidente podremos responder con más velocidad y eficacia.
- Revisa también recurrentemente si el servidor VPN mantiene la privacidad o si puede haber fugas a través de DNS no especificados en la configuración inicial.

Contraseñas y doble factor

Para proteger la información digital de tu organización, es importante que todas las personas cuenten con contraseñas fuertes y seguras, además de activar el doble factor de autenticación.

Con una gestión adecuada de contraseñas es posible disminuir la probabilidad de un incidente de ciberseguridad.

La mejor contraseña es...

- Aquella aleatoria, generada automáticamente por un programa como Dashlane, 1password, Bitwarden y otras.
- Si quieres generar una clave fácil de recordar y difícil de adivinar por otras personas: escoge al azar 4 palabras, ordénalas como prefieras, agrega un par de símbolos de puntuación y usa el texto completo como una clave larga.
- Nunca uses datos como tu dirección, nombres, RUT, teléfono u otros datos personales para generar una clave.

Recomendaciones:

- Los nuevos trabajadores deben seguir las recomendaciones para generar contraseñas seguras. Una vez que finalice un período laboral, elimina accesos de las personas inmediatamente.
- Nunca compartas contraseñas e inicios de sesión con personas que trabajarán por un período determinado.
- Activa el doble factor de autenticación en todas las cuentas de los usuarios.
- Nunca uses la misma contraseña en distintas plataformas.
- Evita claves fáciles de adivinar como: “admin”; “123456” u otras similares.
- Elabora una política para crear contraseñas y difúndela con toda la organización.

Concientización

De acuerdo a cifras entregadas por el Foro Económico Mundial en su último reporte "The Global Risks Report 2022", un "95% de los problemas de ciberseguridad tienen su origen en un error humano" y un "43% de los incidentes de ciberseguridad producidos en las empresas tienen su origen en amenazas internas, intencionales o accidentales".

Estos números revelan la importancia de considerar la educación y concientización en temas de ciberseguridad como un pilar fundamental para evitar y prevenir un incidente de ciberseguridad.

Para esto, es importante elaborar un plan de concientización dirigido a toda la institución durante todo el año.

Para esto, recomendamos:

- ☑ Define un objetivo para tu plan de concientización e indicadores de cumplimiento.
- ☑ Identifica aquellos temas relevantes y las debilidades que tienen como institución.
- ☑ Planifica los temas y haz un calendario para su difusión.
- ☑ Utiliza un lenguaje simple, claro y directo, simple, claro y directo, y asegúrate de que toda la organización lo entienda.
- ☑ Evalúa el impacto de tus campañas y refuerza los temas más relevantes para tu organización.

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

Síguenos