GUÍA DE SEGURIDAD DE TECNOLOGIA INFORMATICA

PROTECCIÓN PARA USTED Y SU TRABAJO

CUMPLIMIENTO DE NORMAS DE SEGURIDAD

Muchos recursos integrales proporcionan orientación sobre la seguridad de la organización (véase el apéndice). Las normas que se enumeran a continuación constituyen un punto de partida para establecer prácticas sólidas de gestión de protección y seguridad. Estas normas no están destinadas a cubrir todos los enfoques o contextos de seguridad y protección, y puede haber situaciones en las que no sea posible cumplir las normas.

Estos materiales se presentan solo para su información. Wellspring no se dedica al negocio de proporcionar servicios de seguridad, y Wellspring no representa a estas prácticas como necesarias, suficientes o apropiadas para cualquier otra organización, ni garantiza que lo sean.

LISTAS DE CONTROL DE NORMAS

SEGURIDAD DE TELÉFONOS MÓVILES

- ○ Siempre agregue una contraseña o PIN a su teléfono.
- ○ Configure su teléfono para que se bloquee automáticamente después de un minuto sin utilizarlo.
- ○ Configure su teléfono para que se desactive solo después de 10 intentos consecutivos de introducir una contraseña incorrecta.
- ○ Agregue la información de su identificación médica (contactos de emergencia, tipo de sangre, etc.) a su teléfono para que sea accesible durante las emergencias desde la pantalla bloqueada.
- ○ Tenga en cuenta que las conversaciones por teléfono móvil son fáciles de monitorear y rastrear. Utilice los servicios de localización solo para aplicaciones de emergencia. Si su ubicación puede poner en peligro a usted y a otras personas, apague el teléfono por completo.
- ○ Evite el uso de SMS (mensajería de texto) para obtener información segura, ya que puede ser fácilmente interceptada.
- ○ Si debe transmitirse información confidencial a través de servicios móviles, utilice una aplicación segura (consulte la sección Comunicaciones seguras).
- ○ Dé a su dispositivo móvil un nombre no descriptivo
- ○ Lleve un registro de sus tarjetas SIM; si fueran robadas, el perpetrador podría hacerse pasar por usted.

MEJORES PRÁCTICAS EN MATERIA DE CONTRASEÑAS

- ○ La creación de contraseñas seguras es una de las partes más importantes para proteger su información.
- ○ Active la autenticación de 2 factores en todas sus cuentas que manejan información confidencial.
- ○ Las contraseñas deben tener al menos 12 caracteres y una mezcla de letras, números y símbolos.
- ○ Un buen consejo es empezar con una frase, quitar los espacios, intencionalmente escribir mal algunas de las palabras y añadir números y símbolos al texto.
- ○ Puede consultar el documento Lineamientos del NIST 2017 sobre prácticas para contraseñas para obtener más información.
- ○ Cambie sus contraseñas frecuentemente, una vez cada 3 meses si es posible.
- ○ Asegúrese de bloquear todos los dispositivos digitales con una contraseña y nunca le dé a nadie su contraseña.

EVITAR VIRUS

- ○ Evite hacer clic en anuncios y enlaces desconocidos.
- ○ Nunca descargue y abra archivos de sitios desconocidos o abra archivos adjuntos de correo electrónico desconocidos.
- ○ No utilice unidades o discos flash desconocidos.
- ○ Evite abrir archivos comprimidos, ya que los analizadores de virus pueden fallar al escanear estos archivos adjuntos a fondo.
- ○ Adopte una herramienta de capacitación sobre conocimientos de seguridad y desarrollar prácticas para educarse a usted y al personal sobre cómo detectar correos electrónicos de phishing.

SEGURIDAD DE LA OFICINA

- ○ Siempre guarde el equipo una vez que haya terminado de usarlo.
- ○ Guarde bajo llave las computadoras y los equipos de servidores importantes para que no estén a la vista.
- ○ Los procedimientos de respuesta médica de emergencia se publican en áreas públicas.
- ○ Manténgase alerta de las personas que miran por encima de su hombro. Minimice la exposición de otras personas a su contenido confidencial.
- ○ Desarrolle y practique regularmente un plan de respuesta a incidentes tanto físicos como de ciberseguridad.
- ○ Las pruebas de desempeño evalúan el cumplimiento del personal de las normas de seguridad y protección.
- ○ Las infracciones de las políticas de seguridad por parte del personal están sujetas a medidas disciplinarias.

GUÍA DE SEGURIDAD DE TECNOLOGIA INFORMATICA

PROTECCIÓN PARA USTED Y SU TRABAJO

SEGURIDAD EN VIAJES

- Mantenga sus dispositivos con usted en todo momento.
- Mantenga sus dispositivos fuera de vista tanto como sea posible.
- Si es posible, evite usar dispositivos en lugares públicos abiertos, ya que nunca se sabe cuándo alguien podría estar escuchando a escondidas.
- Evite discutir temas delicados frente a personas que no conoce.
- Consulte con un experto en viajes y riesgos si planea viajar a un lugar de alto riesgo.

RESPALDOS EN LA NUBE

- Dado que los discos duros para computadoras no son confiables y pueden ser robados, siempre mantenga una copia de seguridad de todos sus archivos en un sitio de buena reputación en la nube.
- Si no es posible el almacenamiento en la nube, utilice una unidad flash encriptada y manténgala en un lugar físicamente seguro.
- Los servicios de nube basados en Internet son los más fiables para realizar copias de seguridad de sus archivos. Algunos de los servicios más comunes son Box, Microsoft Off Ice 365 y Google Drive.
- Confirme que el sitio web que está utilizando para realizar la copia de seguridad de sus archivos contenga “https” en la dirección URL. Esto asegura que los datos que está cargando y descargando estén encriptados en tránsito.

COMUNICACIÓN SEGURA

- Recomendamos la aplicación de fácil uso Signal para móviles para llamados y chats seguros a través de teléfonos móviles.
- Los diferentes programas y aplicaciones ofrecen diferentes niveles de seguridad dependiendo de la encriptación que utilicen.
- Las herramientas más seguras proporcionan encriptación extremo a extremo, como el correo PGP, la mensajería OTR (Off The Record) y la aplicación Signal.
- El correo electrónico, los teléfonos y los mensajes de texto se encuentran entre los métodos de comunicación menos seguros.
- Elija siempre la herramienta más segura que pueda, dados sus recursos actuales.
- En muchos casos, a menudo es mejor pedir ayuda de forma insegura que no pedir ayuda en absoluto.
- Utilice la opción “Copia oculta” (CCO) cuando envíe correos electrónicos a una lista de distribución. Esto ayuda al lector, ya que no tendrá que desplazarse hacia abajo para acceder al nuevo contenido. También oculta a los otros receptores entre sí, lo que a menudo es una necesidad de seguridad.

ACCESO A WIFI

- Los puntos de acceso inalámbricos sin la seguridad adecuada pueden comprometer su red y sus datos.
- Asegúrese de que cualquier enrutador al que se conecte tenga claves WPA o WPA2 con una contraseña segura para evitar que su tráfico sea interceptado.
- Si está creando un punto de acceso wifi, considere la posibilidad de agregar una red de invitados que no esté conectada a la red principal para mayor seguridad.
- Cambie siempre la contraseña de administrador predeterminada en los routers y puntos de acceso inalámbricos de su empresa y de su hogar.

APÉNDICE

- Resistencia y Relisiencia Feminista
- Proteccion Para Los Defensores de Derechos Humanos
- Seguridad en una caja
- Security Planner - Improve your Online Safety
- Holistic Security - A Strategy Manual for Human Rights Defenders
- Workbook on Security: Practical Steps for Human Rights Defenders at Risk
- Insiste, Persiste, Resiste - Women HRD’s Security Strategies
- Front Line Handbook for Human Rights Defenders: What Protection can EU and Norwegian Diplomatic Missions Offer?